CHAPITRE II

Les ordinaux

RÉSUMÉ. • *Un bon ordre est un ordre total tel que toute partie non vide a un plus petit élément. L'ordre des entiers est un bon ordre, pas celui des réels.*
• *Deux bons ordres sont toujours comparables : l'un est isomorphe à un segment initial de l'autre.*
• *Les bons ordres sont munis d'opérations d'addition, de multiplication, et d'exponentiation.*
• *Un ensemble A est dit transitif si tout élément d'un élément de A est dans A.*
• *Un ordinal est défini comme ensemble transitif sur lequel l'appartenance est un bon ordre ; $\emptyset$ est un ordinal, et si α est un ordinal, il en est de même de $S(\alpha) = \alpha \cup \{\alpha\}$, d'où pour chaque entier n, un ordinal $\underline{n} = S^n(\emptyset)$ à n éléments.*
• *Pour α, β ordinaux, on déclare $\alpha < \beta$ vrai si α est élément de β. Alors $<$ est un bon ordre sur les ordinaux ; $S(\alpha)$ est successeur immédiat de α ; tout ensemble non vide d'ordinaux A a un plus petit élément, à savoir $\bigcap A$, et une borne supérieure, à savoir $\bigcup A$.*
• *Aucun ensemble ne contient tous les ordinaux.*
• *Les ordinaux non nuls se partagent en ordinaux successeurs, du type $S(\alpha)$, et ordinaux limites, qui vérifient $\lambda = \bigcup \lambda$. Le plus petit ordinal limite est ω, borne supérieure des ordinaux finis.*
• *Les opérations sur les bons ordres induisent une addition, une multiplication, et une exponentiation sur les ordinaux, qui, via l'identification de n et $\underline{n}$, prolongent celles des entiers. Diverses relations, associativité, distributivité, continuité, etc. sont satisfaites, mais pas toutes celles de l'arithmétique des entiers: on a $\underline{1} + \omega = \omega \cdot \underline{2} = \underline{2}^\omega = \omega$.*

► Ce chapitre décrit la construction d'une famille d'ensembles particuliers, les ordinaux. On montre que les ordinaux sont munis d'un bon ordre canonique, et qu'ils constituent un prolongement transfini de la suite des entiers naturels.

Dans la première partie, on étudie la notion de bon ordre, les opérations de somme, produit, et exponentiation de bons ordres, et on montre le théorème de comparaison affirmant que, de deux bons ordres, l'un est toujours isomorphe à un début de l'autre.

Dans la deuxième partie, on construit les ordinaux comme des ensembles purs particuliers et on en établit les propriétés de base, en particulier le fait que tout bon ordre est isomorphe à un unique ordinal.

Dans la troisième partie, on montre que les ordinaux sont munis d'opérations arithmétiques étendant celles des entiers. Les propriétés algébriques de ces opérations ressemblent à celles des opérations sur les entiers, mais elles en diffèrent dans le domaine transfini ; en particulier, ni l'addition, ni la multiplication ordinale ne sont commutatives.

Dans la quatrième partie, on utilise les ordinaux pour démontrer deux applications, à savoir le théorème de Cantor-Bernstein sur la structure des fermés de $\mathbb{R}$, et le théorème de Goodstein sur la convergence paradoxale des suites arithmétiques du même nom. ◀

▷ *La suite des ordinaux est un prolongement de la suite des entiers naturels au-delà du fini, et elle joue un rôle fondamental dans la théorie des ensembles et plus généralement la logique, rôle comparable à celui de la suite des entiers naturels dans l'ensemble des mathématiques. En particulier, le principe d'induction et la possibilité de définitions récursives s'étendent des entiers aux ordinaux, et tant les démonstrations par induction ordinale que les constructions par récursion ordinale sont omniprésentes dans toute la théorie des ensembles.*

Il existe plusieurs constructions possibles des ordinaux : par exemple, pour Cantor qui les a introduits à la fin du XIXe siècle, un ordinal est une classe d'isomorphisme de bons ordres. Depuis von Neumann dans les années 1920, on sait qu'on peut construire les ordinaux comme une famille de bons ordres particuliers, ce qui revient à choisir un représentant distingué dans chaque classe d'isomorphisme. C'est la construction qu'on suivra ici, car elle offre du plus l'avantage que les ensembles ainsi obtenus sont purs, au sens (encore informel) introduit au chapitre I. On fait ainsi d'une pierre deux coups, en établissant à la fois les propriétés de base des ordinaux, et en commençant à montrer la richesse des ensembles purs, ce qui était une des questions laissées ouvertes à la fin du chapitre I et une des premières tâches à accomplir pour légitimer l'option de restreindre la théorie des ensembles à une théorie des ensembles purs. Les résultats accumulés dans le présent chapitre permettront d'obtenir au chapitre III une réponse définitivement positive, et ainsi d'asseoir sur des bases solides la théorie en construction.

L'approche développée dans ce chapitre est élémentaire, au sens où on ne cherchera pas ici à se raccrocher au contexte axiomatique esquissé à la fin du chapitre I : on raisonne ici dans un contexte mathématique standard, et ce n'est qu'au chapitre III qu'on reviendra sur ces raisonnements pour se demander s'ils entrent ou non dans le cadre de la théorie de Zermelo. ◁

1. Bons ordres

▶ Cette partie contient des généralités sur des ordres totaux particuliers appelés bons ordres. Le résultat principal est le théorème montrant que deux bons ordres sont toujours comparables au sens où l'un est isomorphe à un segment initial de l'autre. On montre aussi que les bons ordres peuvent être composés à l'aide d'opérations naturelles, somme, produit, et, avec quelques difficultés, exponentiation. ◀

▷ *Ce qui légitime les démonstrations par récurrence sur les entiers est la propriété que tout ensemble non vide d'entiers a un plus petit élément. Le principe de récurrence s'étend sans modification à tous les ordres qui ont la même propriété, à savoir que toute partie non vide admet un plus petit élément. Ce sont ces ordres, appelés bons ordres, qu'on étudie ici.* ◁

1.1. Relations bien fondées et bons ordres.

▶ On définit la notion de relation bien fondée, qui est le cadre naturel le plus général pour énoncer un principe d'induction général, puis celle de bon ordre, qui correspond au cas d'un ordre total bien fondé. ◀

▷ *On sait l'importance des démonstrations par récurrence — ou induction — sur les nombres entiers, soit sous la forme locale « si $\mathcal{P}(0)$ est vraie et si $\mathcal{P}(n)$ entraîne $\mathcal{P}(n+1)$ pour tout n, alors $\mathcal{P}(n)$ est vraie pour tout n », soit sous la forme globale équivalente « si, quel que soit n, on a $\mathcal{P}(n)$ dès qu'on a $\mathcal{P}(k)$ pour $k < n$, alors $\mathcal{P}(n)$ est vraie pour tout n ». Dans tous les cas, la validité de la démonstration repose sur l'introduction de l'ensemble A des entiers n ne satisfaisant pas $\mathcal{P}(n)$ et la remarque que l'hypothèse interdit que A ait un plus petit élément : comme toute partie non vide de $\mathbb{N}$ a un plus petit élément, la seule solution est que A soit vide. Ce principe de démonstration s'étend immédiatement à tout ensemble ordonné $(A, \prec)$ possédant, comme $(\mathbb{N}, <)$, la propriété que toute partie non vide a un plus petit élément, et, plus* *généralement, à toute structure (A, R) où R est une relation binaire sur A telle que toute partie non vide de A a un élément R-minimal.* ◁

DÉFINITION 1.1. (bien fondé) Une relation binaire R sur un ensemble A est dite *bien fondée* si toute partie non vide X de A possède un élément R-minimal, c'est-à-dire qu'il existe un élément m de X tel que xRm n'est vérifié pour aucun élément x de X.

EXEMPLE 1.2. La relation d'ordre (stricte) $<$ sur $\mathbb{N}$ est bien fondée. En effet, soit X une partie non vide de $\mathbb{N}$, et soit p un élément quelconque de X. Ou bien p est minimal dans X, ou bien il existe p_1 dans X vérifiant $p_1 < p$. A nouveau, ou bien p_1 est minimal dans X, ou bien il existe p_2 dans X vérifiant $p_2 < p_1$, et ainsi de suite. Par construction, on a $p_1 \leqslant p - 1$, $p_2 \leqslant p - 2$, et, de proche en proche, $p_i \leqslant p - i$. La descente s'arrête donc après au plus p étapes, et il existe donc i au plus égal à p tel que p_i est plus petit élément de X.

Toute relation bien fondée donne lieu à un schéma d'induction :

PROPOSITION 1.3. (induction) *Supposons que R est une relation binaire bien fondée sur un ensemble A, et que $\mathcal{P}(x)$ est une propriété pour laquelle le principe de séparation est valide et telle que, quel que soit x dans A, si $\mathcal{P}(y)$ est vraie pour tous les y vérifiant yRx, alors $\mathcal{P}(x)$ est vraie. Alors $\mathcal{P}(x)$ est vraie pour tout x dans A.*

DÉMONSTRATION. Soit X le sous-ensemble de A formé par les éléments x ne vérifiant pas $\mathcal{P}(x)$ [1]. Si X n'est pas vide, il possède un élément R-minimal m. Soit y un élément de A vérifiant yRm. La minimalité de y entraîne que y n'est pas dans X, c'est-à-dire que $\mathcal{P}(y)$ est vraie. Ceci valant pour tout y vérifiant yRm, l'hypothèse implique que $\mathcal{P}(m)$ est vraie, contredisant le fait que m appartienne à X. La seule possibilité est donc que X soit vide, c'est-à-dire que $\mathcal{P}(x)$ soit vraie pour tout x dans A. □

▷ *Les relations bien fondées et les inductions associées joueront un grand rôle dans toute la suite. Dans ce chapitre, on va se concentrer sur un cas particulier important, à savoir celui des ordres totaux bien fondés.* ◁

CONVENTION 1.4. (ordres) Dans toute la suite, on appelle *ordre* une relation réflexive, antisymétrique et transitive, et on utilise les symboles $\leqslant$, $\preccurlyeq$, $\sqsubseteq$, $\subseteq$, ... pour représenter des ordres. Si $\leqslant$ est un ordre, on note $<$ l'*ordre strict* associé, c'est-à-dire la relation « $x \leqslant y$ et $x \neq y$ », qui est antiréflexive ($x < x$ est toujours faux) et transitive. Inversement, si $<$ est un ordre strict, on utilise $\leqslant$ pour l'ordre (large) associé, c'est-à-dire la relation « $x < y$ ou $x = y$ ». De même pour $\preccurlyeq$ et $\prec$, $\sqsubseteq$ et $\sqsubset$, $\subseteq$ et $\subset$, *etc.*

Un ordre est dit *total* (ou linéaire) si deux éléments quelconques sont comparables, c'est-à-dire si, pour tous a, b dans le domaine concerné, est vérifiée au moins une des relations $a \leqslant b$ ou $b \geqslant a$, et, donc, exactement une des trois relations $a < b$, $a = b$, $a > b$.

[1] c'est ici qu'il faut être sûr qu'un tel ensemble existe, c'est-à-dire qu'on peut séparer dans A les éléments qui satisfont $\mathcal{P}$: se rappeler le paradoxe de Berry

Définition 1.5. (bon ordre) Un ordre $\leqslant$ sur un ensemble A est dit *bon* si toute partie non vide de A possède un plus petit élément (pour $\leqslant$). On dit alors que $(A, \leqslant)$ est un ensemble *bien ordonné*.

Si $<$ est une relation d'ordre strict, on dit que $<$ est un *bon ordre strict* si la relation large associée $\leqslant$ est un bon ordre. En pratique, on emploiera « bon ordre » aussi bien pour l'ordre strict que pour l'ordre large, la notation $<$ ou $\leqslant$ indiquant sans ambiguïté à quelle forme on se réfère.

Le lien entre relation bien fondée et bon ordre est immédiat :

Lemme 1.6. *Pour tout ordre strict $<$ sur A, il y a équivalence entre :*
(i) la relation $<$ est ordre total bien fondé;
(ii) la relation $<$ est un bon ordre (strict).

Démonstration. Supposons que $<$ est un ordre total bien fondé sur A, et soit X une partie non vide de A. Par définition, X possède un élément m tel que, quel que soit x dans X, on n'a pas $x < m$. Comme $<$ est un ordre total, si on n'a pas $x < m$, on doit avoir $m \leqslant x$, et donc m est plus petit élément de X. Par conséquent $<$ est un bon ordre.

Inversement, supposons que $<$ est un bon ordre sur A. D'abord $<$ est total. En effet, si a et b sont deux éléments de A, la partie $\{a, b\}$ a un plus petit élément qui est a ou b, donc on doit avoir $a \leqslant b$ ou $b \leqslant a$. D'autre part, un plus petit élément est toujours minimal: si on a $m \leqslant x$ pour tout x dans X, on a certainement $x \not< m$, puisque $<$ est antisymétrique. Donc toute partie non vide de A possède un élément $<$-minimal, et $<$ est une relation bien fondée. □

Avant même de donner des exemples de bons ordres, et vue son importance pour la suite, on réénonce le principe d'induction [2] spécialisé aux bons ordres :

Proposition 1.7. (induction) *Supposons que $<$ est un bon ordre sur A, et que $\mathcal{P}(x)$ est une propriété pour laquelle le principe de séparation est valide et telle que $\mathcal{P}(x)$ est vraie dès que $\mathcal{P}(y)$ est vraie pour tous y vérifiant $y < x$. Alors $\mathcal{P}(x)$ est vraie pour tout x dans A.*

Exemple 1.8. (bon ordre) L'ordre usuel sur $\mathbb{N}$ est un bon ordre, ainsi qu'on l'a vu ci-dessus. Il résulte de la proposition 1.9 ci-dessous que la restriction de cet ordre à un intervalle fini est aussi un bon ordre, et, de là, que tout ordre total sur un ensemble fini est un bon ordre.

Par contre, il est faux que tout ordre soit un bon ordre : l'ordre usuel sur $\mathbb{Z}$ n'est pas un bon ordre, puisque $\mathbb{Z}$ n'a pas de plus petit élément; de même, l'ordre usuel sur $\mathbb{Q}$ n'est pas un bon ordre puisque la partie $\mathbb{Q}_{>0}$ (rationnels strictement positifs) n'a pas de plus petit élément. D'une façon générale, un ordre dense, c'est-à-dire tel qu'entre deux éléments il y en ait toujours une troisième, n'est jamais bon.

Les propriétés suivantes des bons ordres sont faciles :

Proposition 1.9. (bon ordre) *Soit $(A, <)$ un ensemble bien ordonné.*
(i) S'il est non vide, A possède un plus petit élément, et tout élément de A qui

[2] ou de récurrence, les deux mots étant employés ici comme synonymes

n'est pas maximal possède un plus petit majorant.
(ii) Il n'existe pas de suite infinie strictement décroissante dans $(A, <)$, c'est-à-dire pas de suite $(a_1, a_2, \dots)$ avec $a_1 > a_2 > \dots$.
(iii) Si B est un sous-ensemble de A, alors la restriction de $<$ à B est un bon ordre.

Démonstration. (i) On applique la définition d'un bon ordre à la partie de A constituée de A lui-même, et, pour a non maximal, à la famille des majorants de a.

(ii) Si on a $a_1 > a_2 > \dots$, alors le sous-ensemble $\{a_1, a_2, \dots\}$ de A n'a pas de plus petit élément.

(iii) Si X est une partie non vide de B, alors X a dans A un plus petit élément a, qui, étant dans X, est dans B, donc est plus petit élément de X dans $(B, <)$. $\square$

▷ *Le fait que l'ordre usuel sur les rationnels ou les réels ne soit pas un bon ordre ne prouve pas que d'autres ordres sur ces mêmes ensembles ne puissent pas être des bons ordres : par exemple, puisqu'il existe une bijection f de $\mathbb{N}$ sur $\mathbb{Q}$, on peut définir un ordre exotique sur $\mathbb{Q}$ en déclarant que $x \prec y$ est vrai pour $f^{-1}(x) < f^{-1}(y)$; par construction, $(\mathbb{N}, <)$ et $(\mathbb{Q}, \prec)$ sont isomorphes, et $\prec$ est donc un bon ordre sur $\mathbb{Q}$. Ceci mène à la question ci-dessous. On y reviendra, de même qu'à la question suivante, au chapitre IV :* ◁

Question 1.10. *Existe-t-il un bon ordre sur tout ensemble ?*

Question 1.11. *La condition nécessaire de la proposition 1.9(ii) est-elle suffisante, c'est-à-dire la non-existence d'une suite infinie décroissante pour un ordre total entraîne-t-elle que cet ordre est un bon ordre ?*

1.2. Rigidité des bons ordres.

► On montre qu'un bon ordre est rigide, c'est-à-dire ne possède pas d'automorphisme non trivial. ◄

▷ *La notion de morphisme pertinente pour les ensembles ordonnés est celle d'application strictement croissante : si $(A, <)$ et $(B, \prec)$ sont deux ordres (stricts), une application f de A dans B est dite strictement croissante si $x < y$ entraîne $f(x) \prec f(y)$. Si, de plus, f est bijective, on dit que c'est un isomorphisme de $(A, <)$ sur $(B, \prec)$, ce qui correspond bien à l'idée de deux avatars du même ordre.*

A la différence des ordres totaux généraux qui ont de multiples degrés de liberté, et de là de multiples possibilités d'automorphismes — toute translation est un automorphisme de $(\mathbb{Z}, <)$ — les bons ordres sont des structures très contraintes, dont le seul degré de liberté est la longueur. ◁

On commence par rappeler que, dans le contexte des ordres totaux, toute implication du type « $x < y$ entraîne $f(x) \prec f(y)$ » est une équivalence.

Lemme 1.12. *Soient $(A, <)$ et $(B, \prec)$ deux ensembles ordonnés. Supposons que $<$ est total et que f est une application strictement croissante de A dans B. Alors f est injective, et $x < y$ équivaut à $f(x) \prec f(y)$.*

Démonstration. Supposons $x, y \in A$ avec $x \neq y$: puisque $<$ est total, on a soit $x < y$, soit $y < x$. Dans le premier cas, on déduit $f(x) \prec f(y)$, dans le second, $f(y) \prec f(x)$, et, dans chaque cas, $f(x) \neq f(y)$. Donc f est injective.

Soient maintenant x, y quelconques dans A, et supposons $f(x) \prec f(y)$. Si on n'avait pas $x < y$, on aurait soit $x = y$, qui entraîne $f(x) = f(y)$, soit $y < x$, qui entraîne $f(y) \prec f(x)$, et les deux contredisent $f(x) \prec f(y)$. La seule possibilité est donc $x < y$. $\square$

Le point important pour la rigidité des bons ordres est le fait suivant :

Lemme 1.13. *Soient* $(A, <)$ *un ensemble bien ordonné, et* f *une application strictement croissante de* $(A, <)$ *dans lui-même. Alors, pour tout* a *dans* A*, on a* $a \leqslant f(a)$.

Démonstration. Posons $X = \{x \in A\,;\, f(x) < x\}$. Si A est non vide, X a un plus petit élément, soit m. Puisque m est dans X, on a $f(m) < m$. Comme f est strictement croissante, on déduit $f(f(m)) < f(m)$. D'un autre côté, $f(m)$ n'est pas dans X, puisqu'il est plus petit que le plus petit élément de X. Par définition de X, cela signifie qu'on a $f(f(m)) \not< f(m)$, contredisant ce qui précède. C'est donc que X est vide. □

On en déduit le résultat de rigidité :

Proposition 1.14. (rigidité) *Si* $(A, <)$ *et* $(B, \prec)$ *sont deux ensembles bien ordonnés, il existe au plus un isomorphisme de* $(A, <)$ *sur* $(B, \prec)$*. En particulier, l'identité est le seul automorphisme d'un ensemble bien ordonné.*

Démonstration. Supposons que f et g sont deux isomorphismes de $(A, <)$ sur $(B, \prec)$. Alors, par le lemme 1.12, g^{-1} est strictement croissante, et donc $g^{-1} \circ f$ est une application strictement croissante de $(A, <)$ dans lui-même. Le lemme 1.13 implique $a \leqslant g^{-1} \circ f(a)$ pour tout a dans A, donc, puisque g est croissante, $g(a) \preccurlyeq f(a)$. Un argument symétrique donne de même $f(a) \preccurlyeq g(a)$, donc finalement $f(a) = g(a)$ pour tout a. □

1.3. Comparaison des bons ordres.

► On montre que, de deux bons ordres non isomorphes, l'un est toujours un début de l'autre. ◄

▷ *Il est faux que deux ordres totaux sont toujours comparables au sens où, s'ils ne sont pas isomorphes, l'un est isomorphe à un segment initial de l'autre : par exemple, aucun des deux ordres totaux* $(\mathbb{Z}, <)$*,* $(\mathbb{Q}_{>0}, <)$ *n'est isomorphe à un début de l'autre puisque tout segment initial du premier est discret, alors que tout segment initial du second est dense. Le théorème de comparaison est donc un résultat spécifique aux bons ordres. La démonstration repose sur l'analyse des segments initiaux d'un bon ordre et sur la rigidité.* ◁

Définition 1.15. (segment initial) Supposons que $<$ est un ordre sur A. Pour a dans A, on appelle *segment initial* de $(A, <)$ déterminé par a, et on note $I_<(a)$ — ou, simplement, $I(a)$ — l'ensemble $\{x \in A\,;\, x < a\}$ muni de l'ordre induit par $<$.

▷ *Une relation d'ordre étant transitive, un segment initial d'un ensemble ordonné est toujours clos par minorant, c'est-à-dire qu'un minorant d'un élément de* $I(a)$ *est encore dans* $I(a)$*. L'exemple des coupures dans* $\mathbb{Q}$ *montre qu'il n'y a pas de réciproque en général. Par contre, dans le cas des bons ordres, on a la réciproque.* ◁

Lemme 1.16. *Supposons que* $<$ *est un bon ordre sur* A *et que* X *est un sous-ensemble de* A *clos par minorant. Alors* X *est ou bien* A *entier, ou bien un segment initial de* $(A, <)$.

Démonstration. Soit $Y = A \setminus X$. Ou bien Y est vide, auquel cas on a $X = A$, ou bien Y possède un plus petit élément, soit a. Par hypothèse, $x < a$ entraîne $x \notin Y$, donc $x \in X$, et par conséquent $I(a) \subseteq X$. Inversement, soit $x \in X$. Si on avait $a \leqslant x$, alors, comme X est supposé clos par minorant, on déduirait $a \in X$, contrairement à l'hypothèse $a \in Y$. On doit donc avoir $x < a$, donc $X \subseteq I(a)$, et, finalement, $X = I(a)$. □

Lemme 1.17. *Si $<$ est un bon ordre sur A, alors $(A, <)$ n'est isomorphe à aucun de ses segments initiaux, et deux segments initiaux distincts de $(A, <)$ ne sont jamais isomorphes.*

Démonstration. Soit a un élément de A. Soit f une application de A dans $I(a)$: alors on a $f(a) < a$ par hypothèse, ce qui, par le lemme 1.13, interdit que f soit strictement croissante, et, *a fortiori*, qu'elle soit un isomorphisme.

Soient maintenant a, a' deux éléments distincts de A. On a soit $a < a'$, soit $a' < a$. Supposons par exemple $a < a'$. Alors $I(a')$ est bien ordonné par (la restriction de) $<$, et, comme $<$ est transitive, $I(a)$ est un segment initial de $I(a')$. Le résultat ci-dessus montre alors que $I(a')$ n'est pas isomorphe à son segment initial $I(a)$. □

Proposition 1.18. (comparaison) *Soient $(A, <)$, $(B, \prec)$ deux ensembles bien ordonnés. Alors l'un exactement des trois cas suivants se présente :*
(i) $(A, <)$ et $(B, \prec)$ sont isomorphes;
(ii) $(A, <)$ est isomorphe à un segment initial de $(B, \prec)$;
(iii) $(B, \prec)$ est isomorphe à un segment initial de $(A, <)$.

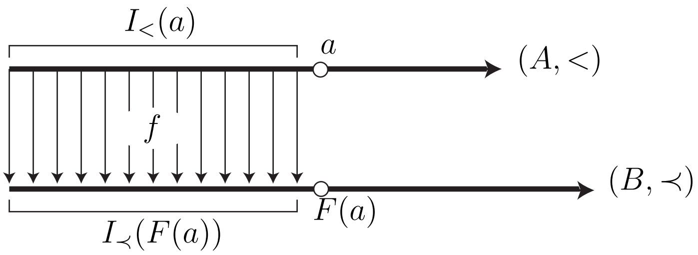


Figure 1. Comparaison de deux bons ordres : on établit une correspondance entre les segments initiaux (c'est-à-dire les débuts) du premier et ceux du second

Démonstration. On définit une correspondance F de A dans B par

$$F(a) = b \Leftrightarrow I_<(a) \text{ est isomorphe à } I_\prec(b)$$

(figure 1). Le lemme 1.17 appliqué à $(B, \prec)$ montre que F est fonctionnelle, c'est-à-dire que, pour chaque a dans A, il existe au plus une valeur b dans B satisfaisant $b = F(a)$. De même, le lemme 1.17 appliqué à $(A, <)$ montre que F est injective, c'est-à-dire que, pour b dans B, il existe au plus une valeur a dans A satisfaisant $b = F(a)$. (Par contre, rien ne prouve que F soit partout définie sur A, ni qu'elle soit surjective.)

Supposons que a appartient au domaine de F, et qu'on a $a' < a$. On va montrer que a' appartient aussi au domaine de F, et qu'on a $F(a') \prec F(a)$. Par définition, il existe un isomorphisme $f : I_<(a) \to I_\prec(F(a))$. Par transitivité de l'ordre $<$, le segment initial déterminé par a' dans $(I_<(a), <)$ est le même que le segment initial $I_<(a')$ qu'il détermine dans $(A, <)$. Soit f' la restriction de f à ce segment initial $I_<(a')$. Par construction, f' est une application strictement croissante de $I_<(a')$ dans $I_\prec(F(a))$. Tout élément x de $I_<(a')$ vérifie $x < a'$, donc

$f'(x) = f(x) \prec f(a')$, ce qui montre que l'image de f' est incluse dans $I_\prec(f(a'))$. Inversement, soit y un élément quelconque de $I_\prec(f(a'))$. Par construction, $f(a')$ est dans $I_\prec(F(a))$, donc y est dans $I_\prec(F(a))$, qui est l'image de f. Il existe donc x dans $I_<(a)$ vérifiant $f(x) = y$. Comme f est un isomorphisme, $y \prec f(a')$ entraîne $x < a'$. C'est dire que y est dans l'image de f', et, par conséquent, f' est un isomorphisme de $I_<(a')$ sur $I_\prec(f(a'))$. Par définition, cela signifie que a' est dans le domaine de F, et qu'on a $F(a') = f(a')$, donc, en particulier, $F(a') \prec F(a)$.

A ce point, on a donc montré que d'une part F est strictement croissante, donc est un isomorphisme de son domaine sur son image, et d'autre part que le domaine de F est clos par minorant dans $(A, <)$.

Un argument symétrique montre que l'image de F est close par minorant dans $(B, \prec)$, c'est-à-dire que, si b appartient à l'image de F, et qu'on a $b' \prec b$, alors b' appartient aussi à l'image de F — et qu'on a $F^{-1}(b') < F^{-1}(b)$, mais ceci est déjà connu.

On applique alors le lemme 1.16. Quatre cas sont *a priori* possibles:

- Cas 1 : $\mathrm{Dom}(F) = A$ et $\mathrm{Im}(F) = B$. C'est dire que $(A, <)$ est isomorphe à $(B, \prec)$.

- Cas 2 : $\mathrm{Dom}(F) = A$ et $\mathrm{Im}(F)$ segment initial de $(B, \prec)$. C'est dire que $(A, <)$ est isomorphe à un segment initial de $(B, \prec)$.

- Cas 3 : $\mathrm{Dom}(F)$ segment initial de $(A, <)$ et $\mathrm{Im}(F) = B$. C'est dire que $(B, \prec)$ est isomorphe à un segment initial de $(A, <)$.

- Cas 4 : $\mathrm{Dom}(F)$ segment initial de $(A, <)$ et $\mathrm{Im}(F)$ segment initial de $(B, \prec)$. Il existe alors a et b tels qu'on ait $\mathrm{Dom}(F) = I_<(a)$ et $\mathrm{Im}(F) = I_\prec(b)$. Mais alors, par construction, F est alors un isomorphisme de $I_<(a)$ sur $I_\prec(b)$: cela signifie qu'on doit avoir $b = F(a)$, donc $a \in \mathrm{Dom}(F)$ et $b \in \mathrm{Im}(F)$, contredisant les hypothèses. Ce cas est donc impossible. □

▷ *La plus grande partie de la démonstration précédente reste valable quand $(A, <)$ et $(B, \prec)$ sont des ensembles (totalement) ordonnés quelconques, mais, faute de pouvoir appliquer le lemme 1.16, on ne peut rien conclure en général. Par exemple, si on part de $(\mathbb{Z}, <)$ et $(\mathbb{Q}^+, <)$, le domaine et l'image de la correspondance F obtenue sont purement et simplement vides: aucun segment initial de $(\mathbb{Z}, <)$ n'est isomorphe à un segment initial de $(\mathbb{Q}^+, <)$.* ◁

1.4. Addition de bons ordres.

▶ On introduit la somme de deux ordres, et on montre que la somme de deux bons ordres est un bon ordre. ◀

▷ *Partant de deux ensembles (bien) ordonnés $\mathcal{A}, \mathcal{B}$, on peut construire divers nouveaux ensembles (bien) ordonnés à l'aide d'opérations simples. Le premier est la somme, qui correspond à l'idée d'une juxtaposition : on place tous les éléments de B après tous les éléments de A, tout en gardant l'ordre relatif des éléments dans chacune des deux composantes. Pour que d'éventuels éléments communs à A et B ne créent pas de problème, on doit supposer les domaines disjoints, ce qu'on assure facilement à l'aide d'une notion convenable d'union disjointe.* ◁

Définition 1.19. (somme disjointe, somme) (*i*) Soient A, B deux ensembles. On définit la *somme disjointe* $A \uplus B$ de A et B par

$$A \uplus B = (A \times \{1\}) \cup (B \times \{2\}).$$

(*ii*) Soient $\mathcal{A}$, $\mathcal{B}$ deux ensembles ordonnés, soit $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$. On appelle *somme* de $\mathcal{A}$ et $\mathcal{B}$, noté $\mathcal{A} + \mathcal{B}$, le couple $(A \uplus B, \sqsubset)$, où $\sqsubset$ est définie par

$$(a, i) \sqsubset (b, j) \Leftrightarrow \begin{cases} (i = j = 1 \text{ et } a < b), \text{ ou} \\ (i = j = 2 \text{ et } a \prec b), \text{ ou} \\ (i = 1 \text{ et } j = 2). \end{cases}$$

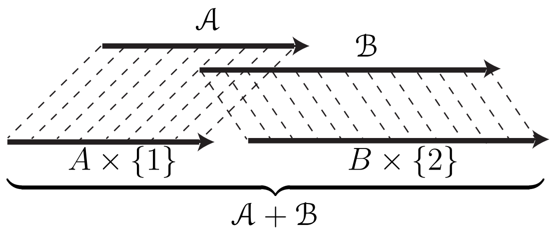


FIGURE 2. Somme de deux ordres $\mathcal{A}, \mathcal{B}$: une copie de $\mathcal{A}$, suivie d'une copie de $\mathcal{B}$; que A et B soient disjoints ou non, les copies $A \times \{1\}$ et $B \times \{2\}$ le sont : par exemple, $A \uplus A$ consiste en deux copies distinctes de A.

EXEMPLE 1.20. (somme) Soient p, q deux entiers. Alors la somme des intervalles $\{1, \ldots, p\}$ et $\{1, \ldots, q\}$, équipés de l'ordre usuel, est isomorphe à l'intervalle $\{1, \ldots, p + q\}$ (équipé de l'ordre usuel).

PROPOSITION 1.21. (somme) *La somme de deux ensembles ordonnés (resp. totalement ordonnés, resp. bien ordonnés) est un ensemble ordonné (resp. totalement ordonné, resp. bien ordonné).*

DÉMONSTRATION. Soient $(A, <)$ et $(B, \prec)$ des ensembles ordonnés. Soit (x, i) un élément quelconque de $A \uplus B$. Pour $i = 1$, on a $(x, i) \not\sqsubset (x, i)$, car ceci équivaudrait à $x < x$, qui est faux puisque $<$ est un ordre. De même, pour $i = 2$, on a $(x, i) \not\sqsubset (x, i)$, car ceci équivaudrait à $x \prec x$, qui est faux puisque $\prec$ est un ordre.

Supposons $(x, i) \sqsubset (y, j) \sqsubset (z, k)$. Par définition, ceci n'est possible que pour $i \leqslant j \leqslant k$. On déduit alors $(x, i) \sqsubset (z, k)$ de ce que $<$ est transitive dans le cas $i = j = k = 1$, de la définition de $\sqsubset$ dans le cas $i < k$, et de la transitivité de $\prec$ dans le cas $i = j = k = 2$. Donc la relation $\sqsubset$ est un ordre strict.

Si à la fois $<$ et $\prec$ sont des ordres totaux, il en est de même de $\sqsubset$: en effet, étant donnés (x, i) et (y, j) quelconques, ou bien on a $i = j = 1$ et alors x et y sont comparables pour $<$, ou bien on a $i = j = 2$, et x et y sont comparables pour $\prec$, ou bien on a $i \neq j$, auquel cas on a soit $i = 1$ et $j = 2$, soit $i = 2$ et $j = 1$.

Supposons enfin que $<$ et $\prec$ sont des bons ordres. Soit X une partie non vide de $A \uplus B$. Deux cas sont possibles. Supposons d'abord $X \cap (A \times \{1\})$ non vide. Comme $<$ est un bon ordre, il existe a dans A tel que $(a, 1)$ est plus petit élément de $X \cap (A \times \{1\})$; comme on a $(a, 1) \sqsubset (y, 2)$ pour tout y dans B, l'élement $(a, 1)$ minore tout élément de $X \cap (B \times \{2\})$, et il est donc plus petit élément de X entier. Supposons ensuite $X \cap (A \times \{1\})$ vide. C'est dire que X est inclus dans $B \times \{2\}$. Comme $\prec$ est un bon ordre, il existe b dans B tel que $(b, 2)$ est plus petit élément de $X \cap (B \times \{2\}$, qui est X. Dans tous les cas, X possède un plus petit élément, et $\sqsubset$ est un bon ordre. $\square$

PROPOSITION 1.22. (associativité) *A isomorphisme près, l'addition des ordres est associative: quels que soient les ensembles ordonnés $\mathcal{A}, \mathcal{B}, \mathcal{C}$, il existe un isomorphisme de $(\mathcal{A} + \mathcal{B}) + \mathcal{C}$ sur $\mathcal{A} + (\mathcal{B} + \mathcal{C})$.*

DÉMONSTRATION. Envoyer $((a, 1), 1)$ sur $(a, 1)$, $((b, 2), 1)$ sur $((b, 1), 2)$, et $(c, 2)$ sur $((c, 2), 2)$. $\square$

1.5. Multiplication de bons ordres.

► On introduit le produit de deux ordres, et on montre que le produit de deux bons ordres est un bon ordre. ◄

⊳ *La seconde opération sur les ordres est la multiplication ordinale, qui consiste à ordonner (anti)-lexicographiquement le produit cartésien. L'intuition est donnée dans la figure 3 : le produit $\mathcal{A} \times \mathcal{B}$ s'obtient en mettant bout à bout des copies (disjointes) de $\mathcal{A}$ indexées par $\mathcal{B}$. On notera que les deux facteurs ne jouent pas le même rôle : dans le produit ici défini, c'est la seconde coordonnée qui est prépondérante.* ⊲

Définition 1.23. (produit) Soient $\mathcal{A}$, $\mathcal{B}$ deux ensembles ordonnés, soit $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$. On appelle *produit* de $\mathcal{A}$ et $\mathcal{B}$, noté $\mathcal{A} \times \mathcal{B}$, le couple $(A \times B, \sqsubset)$, où $\sqsubset$ est définie par

$$(a, b) \sqsubset (a', b') \Leftrightarrow (b \prec b') \text{ ou } (b = b' \text{ et } a < a').$$

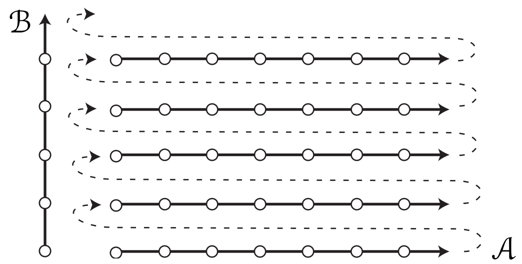


Figure 3. Produit de deux ordres $\mathcal{A}, \mathcal{B}$: $\mathcal{A} \times \mathcal{B}$, c'est $\mathcal{A}$ répété $\mathcal{B}$ fois.

Exemple 1.24. (produit) Soient p, q deux entiers. Alors le produit des intervalles $\{1, \ldots, p\}$ et $\{1, \ldots, q\}$, équipés de l'ordre usuel, est isomorphe à l'intervalle $\{1, \ldots, pq\}$ (équipé de l'ordre usuel).

Proposition 1.25. (produit) *Le produit de deux ensembles ordonnés (resp. totalement ordonnés, resp. bien ordonnés) est un ensemble ordonné (resp. totalement ordonné, resp. bien ordonné).*

Démonstration. Soient $(A, <)$ et $(B, \prec)$ des ensembles ordonnés. Soit (x, y) un élément de $A \times B$. Alors on n'a ni $y \prec y$, ni $y = y$ et $x < x$, donc $(x, y) \sqsubset (x, y)$ est faux, et la relation $\sqsubset$ est antiréflexive.

Supposons $(x, y) \sqsubset (x', y') \sqsubset (x'', y'')$. Quatre cas sont possibles. Si on a $y \prec y' \prec y''$, la transitivité de $\prec$ entraîne $y \prec y''$, donc $(x, y) \sqsubset (x'', y'')$. Si on a $y = y' \prec y''$ ou $y \prec y' = y''$, on obtient $(x, y) \sqsubset (x'', y'')$ directement. Enfin, si on a $y = y' = y''$ et $x < x' < x''$, la transitivité de $<$ entraîne $x \prec x''$, et on a donc $(x, y) \sqsubset (x'', y'')$. Donc la relation $\sqsubset$ est transitive, et c'est un ordre strict sur $A \times B$.

Supposons en outre que $<$ et $\prec$ sont des ordres totaux, et soient (x, y), (x', y') deux éléments distincts de $A \times B$. Si y et y' sont distincts, on a soit $y \prec y'$, soit $y' \prec y$, et, par conséquent, soit $(x, y) \sqsubset (x', y')$, soit $(x', y') \sqsubset (x, y)$. Si y et y' sont égaux, nécessairement x et x' sont distincts, et on a soit $x < x'$, soit $x' < x$, qui impliquent respectivement $(x, y) \sqsubset (x', y')$ ou $(x', y') \sqsubset (x, y)$. Donc la relation $\sqsubset$ est un ordre total sur $A \times B$.

Supposons maintenant que $<$ et $\prec$ sont des bons ordres, et soit X une partie non vide de $A \times B$ (figure 4). La seconde projection $\mathrm{pr}_2(X)$ de X, c'est-à-dire

$$\{y \in B\,;\, \exists x{\in}A\,((x, y) \in X)\},$$

est une partie non vide de B, donc elle admet un plus petit élément, disons b. Alors la fibre en b, c'est-à-dire l'ensemble $\{x \in A\,;\, (x, b) \in X\}$, est une partie non vide de A, donc elle admet un plus petit élément, disons a. Par construction, le couple (a, b) est dans X, et c'en est le plus petit élément. En effet, soit (x, y) un élément quelconque de X. Par construction, on a $y \succcurlyeq b$, donc ou bien $y \succ b$, qui entraîne $(x, y) \sqsupset (a, b)$, ou bien $y = b$. Dans ce dernier cas, on a par construction $x \geqslant a$, et donc $(x, y) \sqsupseteq (a, b)$. □

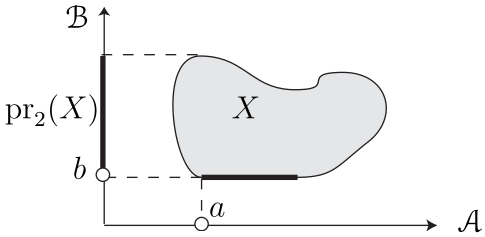


FIGURE 4. Le produit de deux bons ordres est un bon ordre

PROPOSITION 1.26. (associativité, distributivité) *A isomorphisme près, la multiplication des ordres est associative et distributive à gauche par rapport à l'addition: quels que soient les ensembles ordonnés $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, il existe un isomorphisme de $(\mathcal{A}\times\mathcal{B})\times\mathcal{C}$ sur $\mathcal{A}\times(\mathcal{B}\times\mathcal{C})$, et un isomorphisme de $\mathcal{A}\times(\mathcal{B}+\mathcal{C})$ sur $(\mathcal{A}\times\mathcal{B})+(\mathcal{A}\times\mathcal{C})$.*

DÉMONSTRATION. Envoyer $((a, b), c)$ sur $(a, (b, c))$ dans le premier cas, et $(a, (b, 1))$ sur $((a, b), 1)$ et $(a, (c, 2))$ sur $((a, c), 2)$ dans le second. On obtient ainsi deux bijections, et il est facile de vérifier que celles-ci sont strictement croissantes en considérant les différents cas possibles. Ainsi, dans le cas de l'associativité, on a, en notant $<$ tous les ordres, $((a, b), c) < ((a', b'), c')$ si et seulement si soit $c < c'$, soit $c = c'$ et $b < b'$, soit $c = c'$ et $b = b'$ et $a < a'$ est vrai, et c'est aussi le cas de $(a, (b, c)) < (a', (b', c'))$. Dans le cas de la distributivité, $(a, (y, i)) < (a', (y', i'))$ est vrai si on a ou bien $i = i'$ et $y < y'$, ou bien $i = 1$ et $i' = 2$, ou bien $i = i'$ et $y = y'$ et $a < a'$, et c'est aussi le cas pour $((a, y), i) < ((a', y'), i')$ (figure 5). □

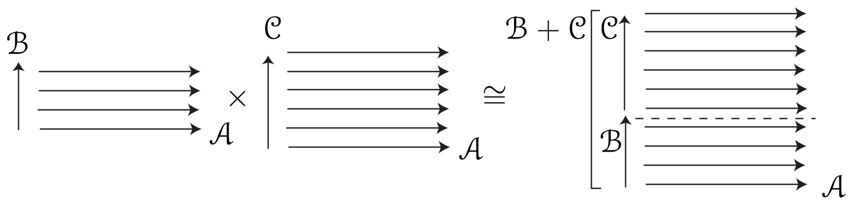


FIGURE 5. Distributivité à gauche de la multiplication des ordres par rapport à l'addition

1.6. Exponentiation de bons ordres.

▶ On introduit une opération d'exponentiation sur les ordres et on montre que l'exponentiation d'un bon ordre par un bon ordre est un bon ordre. ◀

▷ *Pour compléter l'analogie avec les opérations arithmétiques sur les entiers, il est naturel de chercher à définir une opération générale d'exponentiation des ordres consistant à ordonner l'ensemble A^B des suites d'éléments de A indexées par B. Plusieurs solutions sont possibles, mais des difficultés se posent avec les ordres infinis lorsqu'on cherche à ce que l'exponentiation* *de deux bons ordres donne un bon ordre. On est alors amené à restreindre l'ensemble des suites considérées.*

Partant de $\mathcal{A}$, $\mathcal{B}$, avec $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$, on peut déclarer que la suite s est plus petite que la suite t si, pour le $\prec$-plus petit indice i pour lequel on a $s(i) \neq t(i)$, on a $s(i) < t(i)$. Pour assurer l'existence d'un tel plus petit indice i, on suppose que $\prec$ est un bon ordre sur B. Le problème est que, même si $<$ est un bon ordre sur A, et même si A est fini, il est faux que A^B soit bien ordonné dès que B est infini. Par exemple, si $\mathcal{A}$ est $\{0,1\}$ bien ordonné par $0 < 1$ et $\mathcal{B}$ est $\mathbb{N}$ avec l'ordre usuel, on a

$$(1,0,0,0,\dots) > (0,1,0,0,\dots) > (0,0,1,0,\dots) > \dots$$

Le problème est similaire si on prend en compte le plus grand indice où les suites diffèrent. Pour l'éviter, il faudrait que l'ordre sur l'ensemble-exposant soit à la fois un bon ordre et l'opposé d'un bon ordre, c'est-à-dire que toute partie non vide ait à la fois un plus petit et un plus grand élément : ceci caractérise les ensembles finis, et, dans ce cas, on n'obtient rien de plus qu'une itération finie du produit d'ordres.

Le solution trouvée pour échapper à la difficulté précédente consiste à ordonner non pas toutes les suites d'éléments de B indexées par A, mais seulement certaines d'entre elles, dites à support fini. *On verra, en particulier à la fin de ce chapitre avec le théorème de Goodstein, que cette restriction n'enlève pas tout intérêt à l'opération obtenue.* ◁

Définition 1.27. (exponentiation) Soient $\mathcal{A}$, $\mathcal{B}$ deux ensembles ordonnés, soit $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$. On suppose que $\mathcal{A}$ possède un plus petit élément 0.

(i) Pour toute suite s d'éléments de A, on appelle *support* de s l'ensemble $\{i\,;\, s(i) \neq 0\}$, et on note $A^{(B)}$ le sous-ensemble de A^B formé par les suites à support fini.

(*ii*) On appelle *exponentiation* de $\mathcal{A}$ par $\mathcal{B}$, et on note $\mathcal{A}^{\mathcal{B}}$, le couple $(A^{(B)}, \sqsubset)$, où $f \sqsubset g$ est vraie s'il existe i vérifiant $f(i) < g(i)$ et $f(j) = g(j)$ pour $j \succ i$.

▷ *La relation $\sqsubset$ ainsi définie est un ordre anti-lexicographique : on compare les suites en partant des valeurs sur les éléments les plus grands de B, donc en partant de la droite si on voit les éléments de A^B comme des suites d'éléments de A indexées par B.* ◁

Exemple 1.28. Soient p, q deux entiers. Alors l'exponentielle des intervalles $\{1, \dots, p\}$ et $\{1, \dots, q\}$, équipés de l'ordre usuel — par rapport auquel $\{1, \dots, q\}$ a un plus petit élément — est isomorphe à l'intervalle $\{1, \dots, p^q\}$ (équipé de l'ordre usuel).

Proposition 1.29. (exponentiation) *Supposons que $\mathcal{A}$, $\mathcal{B}$ sont deux ensembles totalement (resp. bien) ordonnés, et que $\mathcal{A}$ a un plus petit élément. Alors $\mathcal{A}^{\mathcal{B}}$ est un ensemble totalement (resp. bien) ordonné.*

Démonstration. Supposons $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$. Par définition, on n'a jamais $f \sqsubset f$. Supposons $f \sqsubset g \sqsubset h$. Par définition, il existe i et j dans B tels qu'on ait $f(i) < g(i)$, $f(k) = g(k)$ pour $k \succ i$, et $g(j) < h(j)$, $g(k) = h(k)$ pour $k \succ j$. Puisque $\prec$ est un ordre total, on a ou bien $i \prec j$, ou bien $i = j$, ou bien $i \succ j$. Dans le premier cas, on trouve $f(j) = g(j) < h(j)$, d'où $f(j) < h(j)$, et $f(k) = g(k) = h(k)$ pour $k \succ j$. Dans le second cas, on trouve $f(i) < g(i) < h(i)$, d'où $f(i) < h(i)$, et $f(k) = g(k) = h(k)$ pour $k \succ i$. Enfin, dans le troisième, on trouve $f(i) < g(i) = h(i)$, d'où $f(i) < h(i)$, et $f(k) = g(k) = h(k)$ pour $k \succ i$. On a à chaque fois $f \sqsubset h$, et donc $\sqsubset$ est un ordre strict.

Cet ordre est total : en effet, f et g étant deux éléments quelconques de $A^{(B)}$, l'ensemble des indices i vérifiant $f(i) \neq g(i)$ est inclus dans la réunion des supports de f et g, qui est un ensemble fini, et possède donc un plus grand élément i vis-à-vis de $\prec$. On a alors l'une des deux relations $f(i) \prec g(i)$, $f(i) \succ g(i)$, et donc soit $f \sqsubset g$, soit $f \sqsupset g$.

Supposons maintenant que $<$ et $\prec$ sont des bons ordres, et soit X une partie non vide de $A^{(B)}$. Nous voulons montrer que X possède un plus petit élément. Par hypothèse, chaque fonction f dans $A^{(B)}$ a un support fini; on notera $s_1(f)$ le plus grand élément du support de f vis-à-vis de l'ordre $\prec$, s'il existe, c'est-à-dire si f n'est pas la fonction constante de valeur 0, et, plus généralement, on notera $s_1(f), s_2(f), \ldots$ l'énumération décroissante du support de f. Par définition, pour chaque f, l'élément $s_k(f)$ n'est défini que pour un nombre fini de valeurs de k.

Posons, pour démarrer une induction, $X_0 = X$. Deux cas sont possibles. Ou bien la fonction constante f_0 de valeur 0 est dans X_0, et alors, par définition, f_0 minore tout élément de $A^{(B)}$, donc f_0 est plus petit élément de X_0. Ou bien f_0 n'est pas dans X_0, ce qui signifie que $s_1(f)$ est défini pour chaque fonction dans X_0. Posons

$$\begin{aligned} b_1 &= \inf\{s_1(f)\,;\, f \in X_0\}, \\ a_1 &= \inf\{f(b_1)\,;\, f \in X_0 \text{ et } s_1(f) = b_1\}, \\ X_1 &= \{f \in X_0\,;\, s_1(f) = b_1 \text{ et } f(b_1) = a_1\}. \end{aligned}$$

Comme $\prec$ est un bon ordre, l'élément b_1 existe, et, comme $<$ en est un aussi, l'élément a_1 existe également. L'ensemble X_1 est un sous-ensemble non vide de X_0. Soit f un élément quelconque de $X_0 \setminus X_1$, et g un élément de X_1. Alors, ou bien on a $s_1(f) \succ b_1$, et donc $g(s_1(f)) = 0 < f(s_1(f))$, donc $g \sqsubset f$. Ou bien on a $s_1(f) = b_1$ et $f(b_1) > a_1$, et donc $g(s_1(f)) = g(b_1) = a_1 < f(s_1(f)) = f(b_1)$, d'où à nouveau $g \sqsubset f$. Il en résulte que X_1 est un segment initial de X_0, et donc, pour montrer que X_0 a un plus petit élément, il suffit de montrer que X_1 a un plus petit élément.

A nouveau, deux cas sont possibles. Ou bien la fonction f_1 définie par $f_1(b) = 0$ pour $b \neq b_1$ et $f_1(b_1) = a_1$ est dans X_1, et alors, par construction, f_1 minore toute fonction f vérifiant $s_1(f) = b_1$ et $f(b_1) = a_1$, donc f_1 est plus petit élément de X_1, donc de X_0. Ou bien f_1 n'est pas dans X_1, ce qui signifie que $s_2(f)$ est défini pour chaque fonction dans X_1. On est alors en position d'induction. On pose

$$\begin{aligned} b_2 &= \inf\{s_2(f)\,;\, f \in X_1\}, \\ a_2 &= \inf\{f(b_2)\,;\, f \in X_1 \text{ et } s_2(f) = b_2\}, \\ X_2 &= \{f \in X_1\,;\, s_2(f) = b_2 \text{ et } f(b_2) = a_2\}. \end{aligned}$$

Le même argument que ci-dessus montre que X_2 est un segment initial de X_1, car on ne considère ici que des fonctions f vérifiant $s_1(f) = b_1$ et $f(b_1) = a_1$, donc le point intervenant dans la comparaison est $s_2(f)$. Introduisons la fonction f_2 définie par $f_2(b) = 0$ pour $b \neq b_1, b_2$, $f_2(b_1) = a_1$ et $f_2(b_2) = a_2$. Ou bien f_2 est dans X_2, auquel cas c'en est le plus petit élément, et donc le plus petit élément de X_1, et de X_0, ou bien f_2 n'est pas dans X_2, auquel cas $s_3(f)$ est défini pour tout f dans X_2, et on peut recommencer, construisant ainsi une suite $X_0 \supseteq X_1 \supseteq X_2 \supseteq \ldots$ aussi longtemps qu'on n'a pas trouvé de plus petit élément. Appelons b_i est la valeur commune de $s_i(f)$ pour f dans X_i. Puisque, par définition, il existe au moins une fonction f dans X_i, on a $b_{i-1} = s_{i-1}(f)$ et $b_i = s_i(f)$, d'où $b_{i-1} \succ b_i$. Puisque $\prec$ est un bon ordre, il est impossible que b_i existe pour tout i : cela signifie que, nécessairement, l'induction doit s'arrêter après un nombre fini d'étapes, c'est-à-dire qu'il existe nécessairement un indice i pour lequel X_{i+1} n'existe pas, c'est-à-dire pour lequel la fonction f_i définie par

$$f_i(b) = 0 \text{ pour } b \neq b_1, \ldots, b_i, \quad f(b_1) = a_1, \quad \ldots, \quad f(b_i) = a_i$$

est dans X_i, dont elle est le plus petit élément, ainsi que celui de X_0. $\square$

Proposition 1.30. (distributivité) *Quels que soient les ensembles totalement ordonnés $\mathcal{A}, \mathcal{B}, \mathcal{C}$ tels que $\mathcal{A}$ ait un élément minimal, il existe un isomorphisme de $\mathcal{A}^{\mathcal{B}+\mathcal{C}}$ sur $\mathcal{A}^{\mathcal{B}} \times \mathcal{A}^{\mathcal{C}}$, et un isomorphisme de $\mathcal{A}^{\mathcal{B}\times\mathcal{C}}$ sur $(\mathcal{A}^{\mathcal{B}})^{\mathcal{C}}$.*

Démonstration. On note A, B, C les domaines respectifs de $\mathcal{A}, \mathcal{B}$, et $\mathcal{C}$, et on note tous les ordres $<$. L'élément minimal de A est noté 0. Il s'agit d'associer, de façon bijective, à toute fonction à support fini f de $B \uplus C$ dans A un couple formé d'une fonction à support fini de B dans A et d'une fonction à support fini de C dans A. Ceci est facile : on associe à f d'une part sa restriction $R_1(f)$ à B, et d'autre part sa restriction $R_2(f)$ à C. Comme $B \uplus C$ est construit comme $B \times \{1\} \cup C \times \{2\}$, la définition formelle est $R_1(f)(b) = f((b, 1))$ pour $b \in B$, et $R_2(f)(c) = f((c, 2))$ pour $c \in C$ La vérification du fait que l'application $F : f \mapsto (R_1(f), R_2(f))$ est une bijection et est strictement croissante est facile (*cf.* figure 6).

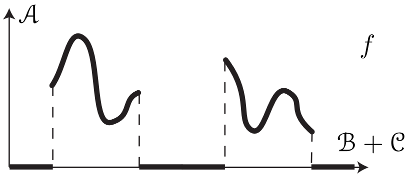


Figure 6. Isomorphisme de $\mathcal{A}^{\mathcal{B}+\mathcal{C}}$ sur $\mathcal{A}^{\mathcal{B}} + \mathcal{A}^{\mathcal{C}}$: on coupe la suite en deux fragments

Pour le second résultat, le principe est le même. Il s'agit cette fois d'associer à toute fonction à support fini f de $B \times C$ dans A une fonction à support fini $F(f)$ de C dans les fonctions à support fini de B dans A. Comme l'élément minimal de A^B est la fonction constante c_0 de valeur 0, être de support fini pour une fonction de C dans A^B signifie prendre la valeur c_0 sauf pour un nombre fini de valeurs. Ici f est une fonction à deux variables, et on définit $F(f)$ en posant $F(f)(c)(b) = f(b, c)$, c'est-à-dire en séparant les deux variables[3]. Comme l'ensemble des couples (b, c) vérifiant $f(b, c) \neq 0$ est fini, l'ensemble des c vérifiant $F(f)(c) \neq c_0$ est fini, et F appartient à $(A^{(B)})^{(C)}$ comme escompté. A nouveau les vérifications requises, à savoir que F est bijective et strictement croissante, sont faciles (*cf.* figure 7). $\square$

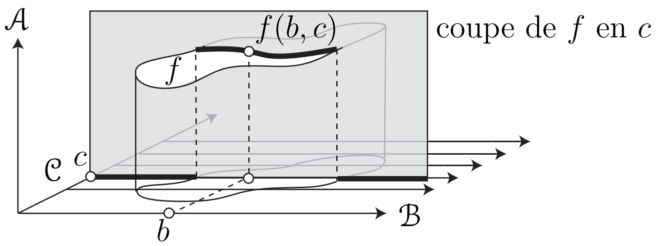


Figure 7. Isomorphisme de $\mathcal{A}^{\mathcal{B}\times\mathcal{C}}$ sur $(\mathcal{A}^{\mathcal{B}})^{\mathcal{C}}$: on associe à une suite f la suite de ses coupes suivant la seconde variable

[3]opération appelée « curryfication » en lambda-calcul

2. Construction des ordinaux

▶ On construit une famille d'ensembles bien ordonnés particuliers, appelés les ordinaux. On montre que les ordinaux se rangent eux-mêmes en une suite bien ordonnée, commençant par une copie de la suite des entiers naturels, mais ne formant pas un ensemble, et que tout ensemble bien ordonné est isomorphe à un unique ordinal. ◀

▷ *La construction décrite ci-dessous, qui est due à John von Neumann, a deux aspects d'importance inégale. Le résultat important est l'existence d'une suite prolongeant indéfiniment la suite des entiers naturels et dotée de diverses bonnes propriétés comme la possibilité d'effectuer des démonstrations inductives. Le point secondaire est que, dans l'approche retenue, les ordinaux se trouvent être des ensembles purs particuliers, et que l'ordre des ordinaux se trouve coïncider avec la relation d'appartenance* $\in$. *Ce dernier point jouera un rôle non négligeable au chapitre III pour mener à bien le programme de représentation des entiers par des ensembles purs, mais, quant au fond, il ne s'agit que d'une astuce de construction: d'autres constructions des ordinaux sont possibles, à commencer par celle de Cantor qui les définissait simplement comme classe d'isomorphisme de bons ordres. Il est certainement plus commode techniquement de travailler avec des représentants distingués qu'avec les classes elles-mêmes, mais le prix à payer est le caractère relativement artificiel de la construction. Les ordinaux qui sont ici introduits par une définition explicite mais assez mystérieuse. Il est conseillé de ne pas trop se focaliser sur cette définition contingente, mais simplement de se convaincre qu'elle mène bien aux propriétés souhaitées, à savoir que les ordinaux forment une suite bien ordonnée et que chaque ensemble bien ordonné est isomorphe à un unique ordinal.* ◁

2.1. Ensembles transitifs.

▶ Avant d'introduire les ordinaux, on introduit les ensembles transitifs, qui sont les ensembles dont tous les éléments des éléments sont éléments. ◀

DÉFINITION 2.1. (transitif) Un ensemble d'ensembles A est dit *transitif* si tout élément d'un élément de A est élément de A, c'est-à-dire si l'ensemble $\bigcup A$ est inclus dans A.

Ainsi, un ensemble A est transitif si et seulement si on a

$$x \in a \in A \Rightarrow x \in A, \tag{2.1}$$

c'est-à-dire encore si $a \in A$ entraîne $a \subseteq A$, donc encore, de façon équivalente, si on a $A \subseteq \mathfrak{P}(A)$.

▷ *La notion d'ensemble transitif n'est pas familière, et il semble clair que la plupart des ensembles ne sont pas transitifs. Cependant on va voir qu'il existe des ensembles transitifs.* ◁

LEMME 2.2. (i) *L'ensemble vide est transitif.*
(ii) *Si A est transitif, il en est de même de $A \cup \{A\}$, de $\mathfrak{P}(A)$, et de $\bigcup A$.*
(iii) *Toute union et toute intersection d'ensembles transitifs est transitive.*

DÉMONSTRATION. (i) Comme $\emptyset$ n'a pas d'élément, l'implication (2.1) est vérifiée.

(ii) Supposons A transitif. Supposons d'abord $x \in a \in A \cup \{A\}$. On a donc $a \in A$ ou $a = A$ (ou les deux). Dans le premier cas, on obtient $x \in a \in A$, donc $x \in A$ puisque A est transitif; dans le second cas, on a $x \in a = A$, donc $x \in A$ directement. Dans tous les cas, on a $x \in A$ et, *a fortiori*, $x \in A \cup \{A\}$. Par conséquent $A \cup \{A\}$ est transitif.

Supposons maintenant $x \in a \in \mathfrak{P}(A)$, soit $x \in a \subseteq A$. Par définition de l'inclusion, ceci entraîne $x \in A$, donc, par (2.1), $x \subseteq A$, soit $x \in \mathfrak{P}(A)$. Par conséquent, $\mathfrak{P}(A)$ est transitif.

Supposons ensuite $x \in a \in \bigcup A$. Par définition, il existe b dans A tel qu'on ait $a \in b \in A$, donc $a \in A$ puisque A est transitif et, de là, $x \in \bigcup A$. Par conséquent, $\bigcup A$ est transitif.

(*iii*) Soit $(A_i)_{i\in I}$ une famille d'ensembles transitifs. Supposons $x \in a \in \bigcup_{i\in I} A_i$. Il existe donc i tel qu'on ait $x \in a \in A_i$, d'où $x \in A_i$ puisque A_i est transtif, et de là $x \in \bigcup_{i\in I} A_i$. Par conséquent $\bigcup_{i\in I} A_i$ est transitif.

Enfin, supposons $x \in a \in \bigcap_{i\in I} A_i$. Pour tout i dans I, on a $x \in a \in A_i$, d'où $x \in A_i$ puisque A_i est transtif, et de là $x \in \bigcap_{i\in I} A_i$. Par conséquent $\bigcap_{i\in I} A_i$ est transitif. □

▷ *Il existe donc une infinité d'ensembles transitifs, puisqu'au moins tous les ensembles inductivement obtenus à partir de l'ensemble vide en utilisant de façon répétée les opérations* $A \mapsto \mathfrak{P}(A)$ *ou* $A \mapsto A \cup \{A\}$ *sont transitifs.*

On notera qu'affirmer qu'une famille $\{A_i\,;\, i \in I\}$ *est transitive et affirmer que chaque élément* A_i *de cette famille est un ensemble transitif sont des conditions distinctes : dans le premier cas, il s'agit de dire que tout élément d'un* A_i *est un* A_j*, alors que, dans le second, il s'agit de dire que tout élément d'un élément d'un* A_i *est élément de cet* A_i*. Les résultats des points* (*ii*) *et* (*iii*) *du lemme 2.2 sont donc disjoints.* ◁

2.2. Ordinaux.

► On introduit les ordinaux comme des ensembles transitifs particuliers, définis en termes de propriétés de la restriction de l'appartenance. ◄

▷ *Pour tout ensemble A, la restriction de la relation d'appartenance à A est une relation binaire sur A. En général, cette relation est purement et simplement vide : il y a a priori aucune raison pour que, parmi les éléments de A, il en existe deux, disons a et b, tels que b soit un ensemble et qu'on ait* $a \in b$*. Cependant, typiquement si A est un ensemble transitif puisqu'alors tout élément d'un élément de A est élément de A, il se peut qu'un élément de A appartienne à un autre élément de A. Par exemple, l'ensemble* $\mathfrak{P}(\mathfrak{P}(\emptyset))$ *a deux éléments, à savoir* $\emptyset$ *et* $\{\emptyset\}$*, et le premier est un élément du second, donc la restriction de* $\in$ *à* $\mathfrak{P}(\mathfrak{P}(\emptyset))$ *se compose de l'unique couple* $(\emptyset, \{\emptyset\})$*. La figure 8 donne un autre exemple.*

Même lorsque la restriction de l'appartenance à un ensemble A est non vide, il n'y a aucune raison pour que cette restriction soit une relation d'ordre, ou une relation d'équivalence, ou quelque relation particulière que ce soit. Cependant, on peut toujours considérer ceux des ensembles A pour lesquels la restriction à A de l'appartance a telle ou telle propriété par exemple d'être un ordre. ◁

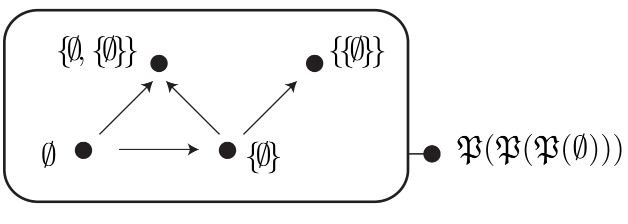


FIGURE 8. Un exemple d'ensemble A tel que la restriction de $\in$ à A ne soit pas vide : l'ensemble $\mathfrak{P}(\mathfrak{P}(\mathfrak{P}(\emptyset)))$

DÉFINITION 2.3. (ordinal) On dit qu'un ensemble α est un *ordinal* si α est un ensemble transitif et que la restriction de $\in$ à α est un bon ordre strict.

Autrement dit, α est un ordinal si les quatre conditions suivantes sont vérifiées:
(i) pour tout x dans α, on a $x \subseteq \alpha$;
(ii) pour tout x dans α, on a $x \notin x$;
(iii) pour tous x, y, z dans α, si on a $x \in y$ et $y \in z$, alors on a $x \in z$;
(iv) pour tout sous-ensemble non vide A de α, il existe x dans A vérifiant $x \in y$ pour tout y dans A distinct de x.

Dans toute la suite, on se conforme à l'usage d'utiliser les minuscules grecques pour les ordinaux, et de les réserver à cette fin.

▷ *Comme pour les ensembles transitifs, il n'est pas a priori évident qu'il existe des ordinaux, et on commence donc par vérifier que c'est bien le cas.* ◁

Lemme 2.4. (i) *L'ensemble vide est un ordinal.*
(ii) *Si α est un ordinal, alors on a $\alpha \notin \alpha$.*
(iii) *Si α est un ordinal, alors on a $\alpha \cup \{\alpha\}$ en est un aussi.*

Démonstration. (i) Comme $\emptyset$ n'a aucun élément, et, de là, aucun sous-ensemble non vide, les quatre conditions qui définissent un ordinal sont automatiquement satisfaites.

(ii) Par définition, si α est un ordinal, on a $x \notin x$ pour tout élement x de α. Si on avait $\alpha \in \alpha$, c'est-à-dire si α était élément de lui-même, on aurait donc $\alpha \notin \alpha$, ce qui contredit l'hypothèse.

(iii) Soit α un ordinal, et $\beta = S(\alpha) = \alpha \cup \{\alpha\}$. Il s'agit de vérifier que β satisfait aux quatre conditions de la définition d'un ordinal. Le lemme 2.2 affirme déjà que $S(\alpha)$ est un ensemble transitif.

Supposons $x \in \beta$. Alors, par définition, on a ou bien $x \in \alpha$, ou bien $x = \alpha$, les deux s'excluant en vertu de (ii). Dans le premier cas, on a $x \notin x$ puisque α est un ordinal, dans le second, on a $x \notin x$ par (ii).

Supposons maintenant $x, y, z \in \beta$, avec $x \in y \in z$. Si x, y et z appartiennent à α, alors on déduit $x \in z$ de l'hypothèse que α est un ordinal. Supposons $x = \alpha$. Par (ii), on ne peut avoir $y = \alpha$, et on a donc $\alpha \in y \in a$. Comme α est un ensemble transitif, cela entraîne $\alpha \in \alpha$, contredisant (ii) : l'hypothèse $x = \alpha$ est donc impossible. Supposons maintenant $y = \alpha$. Nous déduisons alors $z \neq \alpha$, donc $z \in \alpha$, soit $\alpha \in z \in \alpha$, et, à nouveau, $\alpha \in \alpha$: l'hypothèse $y = \alpha$ est donc également impossible. Reste le cas $z = \alpha$. On a alors $x \in y \in \alpha$, et l'hypothèse que α est un ensemble transitif entraîne $x \in \alpha$, soit $x \in z$. On a donc montré dans tous les cas que la restriction de $\in$ à β est une relation transitive.

Soit A un sous-ensemble non vide de β. Supposons d'abord que $A \cap \alpha$ est non vide. Puisque α est un ordinal, il existe x dans $A \cap \alpha$ vérifiant $x \in y$ pour tout y distinct de x dans $A \cap \alpha$. Puisque x est dans $A \cap \alpha$, on a $x \in \alpha$ par hypothèse, et donc $x \in y$ pour tout y distinct de x dans A. Finalement, si A est non vide et $A \cap \alpha$ l'est, comme β est $\alpha \cup \{\alpha\}$, la seule possibilité est $A = \{\alpha\}$. Posons $x = \alpha$: alors x est bien un élément de A vérifiant $x \in y$ pour tout élément de A distinct de x, puisqu'il n'existe pas de tel élément y. □

Il existe donc une infinité d'ordinaux, à savoir au moins $\emptyset$ et tous les ensembles obtenus à partir de $\emptyset$ en répétant l'opération $\alpha \mapsto \alpha \cup \{\alpha\}$.

Notation 2.5. (opération S, ordinal $\underline{n}$) Pour tout ensemble A, on pose $S(A) = A \cup \{A\}$. Pour n entier naturel, on note $\underline{n}$ l'ordinal $S^n(\emptyset)$.

Par exemple, on trouve :
$\underline{0} = \emptyset$,

$\underline{1} = S(\underline{0}) = \{\underline{0}\}$,
$\underline{2} = S(\underline{1}) = \underline{1} \cup \{\underline{1}\} = \{\underline{0}\} \cup \{\underline{1}\} = \{\underline{0}, \underline{1}\}$,
$\underline{3} = S(\underline{2}) = \underline{2} \cup \{\underline{2}\} = \{\underline{0}, \underline{1}\} \cup \{\underline{2}\} = \{\underline{0}, \underline{1}, \underline{2}\}$, *etc.*

On constate sur ces exemples que les éléments de l'ordinal $\underline{n}$ se trouvent être des ordinaux, et plus précisément les ordinaux $\underline{k}$ pour $k < n$. Cette propriété est générale :

Proposition 2.6. (ordinaux $\underline{n}$) *Pour tout entier n, l'ordinal $\underline{n}$ a exactement n éléments, à savoir les ordinaux $\underline{k}$ pour $k < n$.*

Démonstration. On raisonne par récurrence sur n. Pour $n = 0$, c'est-à-dire pour $\emptyset$, le résultat est vrai. Supposons $n > 0$, et posons $m := n - 1$. On a alors $\underline{n} = \underline{m} \cup \{\underline{m}\}$, donc les éléments de $\underline{n}$ sont d'une part les éléments de $\underline{m}$, c'est-à-dire, par hypothèse de récurrence, les m ordinaux $\underline{k}$ avec $k < m$, d'autre part l'unique élément de $\{\underline{m}\}$, c'est-à-dire $\underline{m}$, dont on sait par le lemme 2.4(ii) qu'il n'appartient pas à $\underline{m}$. Donc $\underline{n}$ a n éléments et ce sont les ordinaux $\underline{k}$ avec $k < n$. $\square$

On note deux résultats valables pour tous les ordinaux, qu'ils soient du type $\underline{n}$ ou non :

Lemme 2.7. *(figure 9) Tout élément d'un ordinal α est un ordinal strictement inclus dans α.*

Démonstration. Soit α un ordinal, et x un élément de α. Puisque α est transitif, $x \in \alpha$ implique $x \subseteq \alpha$. On veut montrer que x est un ordinal. Supposons d'abord $z \in y \in x$. Puisque x est inclus dans α, on déduit $y \in \alpha$, puis $z \in \alpha$ puisque α est transitif. Puisque la restriction de $\in$ à α est une relation transitive et que z, y, et x sont éléments de α, on déduit $z \in x$, et x est un ensemble transitif.

Puisque x est inclus dans α, la relation $\in\restriction_x$ est la restriction à x de $\in\restriction_\alpha$, donc, par la proposition 1.9, cette restriction est un bon ordre. Par conséquent, x est un ordinal.

Finalement, on a vu que x est inclus dans α. L'inclusion est stricte, car, par le Lemme 2.4(ii), x est dans α mais pas dans x. $\square$

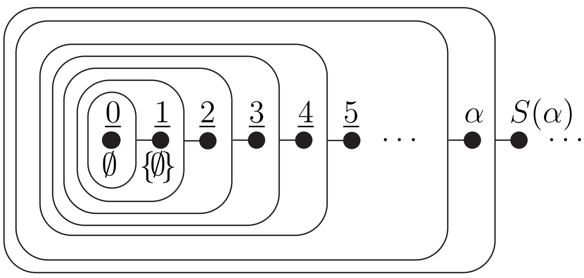


Figure 9. Structure des ordinaux : chaque ordinal α est lui-même un ensemble d'ordinaux inclus dans α ; l'ordinal $S(\alpha)$ est la réunion de α et de $\{\alpha\}$: ses éléments sont donc les éléments de α, ainsi qu'α lui-même

Si A est un ensemble non vide d'ensembles, on note $\bigcap A$ l'*intersection* de A, c'est-à-dire l'ensemble des éléments qui sont dans tous les éléments de A.

Lemme 2.8. *Si A est un ensemble non vide d'ordinaux, $\bigcap A$ est un ordinal.*

Démonstration. Posons $a = \bigcap A = \{\beta\,;\, \forall\alpha{\in}A\,(\beta \in \alpha)\}$. Par hypothèse, tout élément de A est un ordinal, donc est transitif, donc, par le lemme 2.2(iii), l'ensemble a est transitif. Soit α un élément quelconque de A. D'abord tout élément de a est élément de α, donc est un ordinal. Soient β, γ, δ des éléments de a, donc de α. Par le lemme 2.4(ii), on a $\beta \notin \beta$. Ensuite, si on a $\beta \in \gamma \in \delta$, le fait que α soit un ordinal entraîne $\beta \in \delta$. Donc la restriction de $\in$ à a est un ordre strict. Enfin, soit X une partie non vide de a. Alors X est une partie non vide de α, donc elle possède un plus petit élément β vis-à-vis de $\in\restriction_\alpha$, c'est-à-dire qu'on a $\beta \in \gamma$ ou $\beta = \gamma$ pour tout élément γ de X. Ceci signifie que β est plus petit élément de X vis-à-vis de $\in\restriction_a$. Donc la relation $\in\restriction_a$ est un bon ordre, et par conséquent a est un ordinal. □

2.3. L'ordre sur les ordinaux.

► On vient de voir que tous les éléments d'un ordinal sont des ordinaux. On montre ici une sorte de réciproque, à savoir que, si α et β sont des ordinaux distincts et que α n'est pas élément de β, alors nécessairement β est élément de α. Cette propriété permet de construire un ordre total, et même un bon ordre, sur les ordinaux; on en tire un schéma d'induction sur les ordinaux. ◄

Lemme 2.9. *La restriction de la relation $\in$ aux ordinaux est un ordre strict.*

Démonstration. Le lemme 2.4(ii) affirme que $\alpha \in \alpha$ est impossible pour tout ordinal α. Par ailleurs, si α, β, γ vérifient $\alpha \in \beta \in \gamma$, alors, puisque, par définition, γ est un ensemble transitif, on a $\alpha \in \gamma$. Donc la restriction de $\in$ aux ordinaux est antiréflexive et transitive: c'est un ordre strict. □

Définition 2.10. (ordre) Si α, β sont des ordinaux, on dit que α est *plus petit* que β, noté $\alpha < \beta$, si α est élément de β.

Exemple 2.11. Par construction, on a toujours $\alpha \in S(\alpha)$ et donc, puisque $S(\alpha)$ est un ordinal, on a $\alpha < S(\alpha)$. En particulier, on a $\underline{n} < \underline{n+1}$ pour tout entier n. Plus généralement, la proposition 2.6 montre que, pour m, n entiers, $\underline{m} < \underline{n}$ équivaut à $m < n$.

Proposition 2.12. (ordre) (i) *Tout ordinal coïncide avec l'ensemble des ordinaux plus petits que lui.*
(ii) *L'ordre large associé à la restriction de $\in$ aux ordinaux est l'inclusion : si α, β sont des ordinaux, $\alpha \subseteq \beta$ est vrai si et seulement si on a soit $\alpha \in \beta$, soit $\alpha = \beta$ — autrement dit, $\alpha \in \beta$ équivaut à $\alpha \subsetneqq \beta$.*
(iii) *Pour chaque ordinal α, l'ordinal $S(\alpha)$ est succeseur immédiat de α : on a $\alpha < S(\alpha)$, et $\alpha < \beta$ entraîne $S(\alpha) \leqslant \beta$. De plus, S est strictement croissante: $\alpha < \beta$ entraîne $S(\alpha) < S(\beta)$.*

Démonstration. (i) Soit α un ordinal quelconque. Alors α est l'ensemble de ses éléments. Par le lemme 2.7, ceux-ci sont des ordinaux, donc α est l'ensemble des ordinaux qui sont éléments de α: par définition, c'est donc l'ensemble des ordinaux plus petits que α.

(ii) Supposons $\alpha \leqslant \beta$. Nous avons ou bien $\alpha < \beta$, donc, par définition, $\alpha \in \beta$, ce qui, puisque β est transitif, entraîne $\alpha \subseteq \beta$, ou bien $\alpha = \beta$, donc aussi $\alpha \subseteq \beta$. Dans tous les cas, $\alpha \leqslant \beta$ entraîne $\alpha \subseteq \beta$.

Inversement, supposons $\alpha \subseteq \beta$. Alors on a ou bien $\alpha = \beta$, donc $\alpha \leqslant \beta$, ou bien $\alpha \subsetneqq \beta$. Dans ce cas, $\beta \setminus \alpha$ est une partie non vide de α et, puisque $(\beta, \in\restriction_\beta)$ est un ensemble bien ordonné, cette partie $\beta \setminus \alpha$ possède un plus petit élément α', qui est un ordinal comme tout élément de β. On va montrer $\alpha' = \alpha$, qui, puisque α' est dans β, donne $\alpha \in \beta$, donc $\alpha < \beta$, d'où *a fortiori* $\alpha \leqslant \beta$.

Soit $\gamma \in \alpha$ quelconque. Puisque α est inclus dans β, on a $\gamma \in \beta$, et γ est comparable avec α' : l'une des trois relations $\gamma \in \alpha'$, $\gamma = \alpha'$, $\alpha' \in \gamma$ est vraie. Or $\gamma = \alpha'$ donnerait $\gamma \notin \alpha$ puisque α' est dans $\beta \setminus \alpha$, contredisant l'hypothèse $\gamma \in \alpha$. De même, puisque α est un ensemble transitif, $\alpha' \in \gamma$ entraînerait $\alpha' \in \alpha$, contredisant le fait que α' est dans $\beta \setminus \alpha$. On a donc nécessairement $\gamma \in \alpha'$, donc $\alpha \subseteq \alpha'$.

Inversement, supposons $\gamma \in \alpha'$. Puisque β est un ensemble transitif, γ est dans β, et alors la définition de α' comme plus petit élément de $\beta \setminus \alpha$ entraîne $\gamma \in \alpha$. On a donc $\alpha' \subseteq \alpha$, et, finalement $\alpha' = \alpha$, comme annoncé.

(*iii*) La relation $\alpha \in S(\alpha)$, c'est-à-dire $\alpha < S(\alpha)$, est vraie par définition. Supposons $\alpha < \beta$. On a alors $\alpha \in \beta$, donc $\{\alpha\} \subseteq \beta$, et, d'autre part, $\alpha \leqslant \beta$ donc, par (*ii*), $\alpha \subseteq \beta$. On a donc $\alpha \cup \{\alpha\} \subseteq \beta$, soit, toujours par (*ii*), $S(\alpha) \leqslant \beta$. Par ailleurs, on vient de voir que $\alpha < \beta$ entraîne $S(\alpha) \leqslant \beta < S(\beta)$, d'où $S(\alpha) < S(\beta)$. □

L'ordre des ordinaux est un bon ordre au sens suivant :

PROPOSITION 2.13. (bon ordre) *Tout ensemble non vide d'ordinaux A possède un plus petit élément, à savoir $\bigcap A$.*

DÉMONSTRATION. Posons $\alpha = \bigcap A$. Par le lemme 2.8, α est un ordinal. Par construction, on a $\alpha \subseteq \beta$ pour tout β dans A, soit, par la proposition 2.12(*ii*), $\alpha \leqslant \beta$. Supposons que, pour tout β dans A, on a $\alpha < \beta$, c'est-à-dire $\alpha \in \beta$. Alors, par définition, on $\alpha \in \bigcap A$, soit $\alpha \in \alpha$, contredisant le lemme 2.4(*ii*). La seule possibilité est donc qu'il existe β dans A pour lequel on a $\alpha = \beta$, c'est-à-dire que α appartient à A, et donc α est plus petit élément de A. □

Appliquant ce qui précède à la paire $\{\alpha, \beta\}$, on déduit :

COROLLAIRE 2.14. *Pour chaque paire d'ordinaux $\{\alpha, \beta\}$, l'une exactement des trois relations $\alpha \in \beta$, $\alpha = \beta$, $\beta \in \alpha$ est vérifiée.*

▷ *Autrement dit, l'ordre des ordinaux est un ordre total. En vertu de la proposition 2.12(i), le segment initial de la suite des ordinaux déterminé par un ordinal α, c'est-à-dire l'ensemble des ordinaux plus petits que α, coïncide avec α : cette propriété peu intuitive résulte de la définition des ordinaux choisie. A ce point, nous pouvons commencer à représenter la suite des ordinaux comme sur la figure 10 : il s'agit d'une suite totalement ordonnée, $\underline{0}$ en est le plus petit élément, et chaque ordinal α a un successeur immédiat qui est $S(\alpha)$, de sorte que $\underline{1}$ est le second élément, $\underline{2}$ le troisième, etc.* ◁

FIGURE 10. La suite des ordinaux (1) : cette figure est analogue à la figure 9, mais on oublie la structure interne des ordinaux pour ne retenir que leur ordre

▷ *Comme la collection des ordinaux — on évite de dire l'ensemble, on va voir sous peu qu'il n'existe pas d'ensemble de tous les ordinaux — est bien ordonnée, il est immédiat qu'on peut mimer la proposition 1.7 et énoncer un principe d'induction sur les ordinaux. Vue son importance cruciale dans toute la suite, on réénonce le résultat dans le cas spécifique. Noter qu'il y a deux versions, suivant qu'on considère tous les ordinaux, ou simplement les ordinaux plus petits qu'un ordinal donné.* ◁

Proposition 2.15. (induction) *Soit $\mathcal{P}(\alpha)$ une propriété pour laquelle le principe de séparation est valide* [4].

(i) *Supposons que, pour tout α plus petit que θ, la propriété $\mathcal{P}(\alpha)$ est vraie dès que $\mathcal{P}(\beta)$ l'est pour $\beta < \alpha$. Alors $\mathcal{P}(\alpha)$ est vraie pour tout ordinal α plus petit que θ.*

(ii) *Supposons que $\mathcal{P}(\alpha)$ est vraie dès que $\mathcal{P}(\beta)$ l'est pour $\beta < \alpha$. Alors $\mathcal{P}(\alpha)$ est vraie pour tout ordinal α.*

Démonstration. Le point (i) est l'application de la proposition 1.7 à l'ensemble bien ordonné $(\theta, <)$. Pour (ii), on redonne un argument direct —- faute de pouvoir parler de l'ensemble de tous les ordinaux. Supposons qu'il existe un ordinal α tel que $\mathcal{P}(\alpha)$ soit fausse. Soit $X := \{\beta \in \alpha\,;\, \mathcal{P}(\beta) \text{ est fausse}\}$. L'hypothèse de séparation sur $\mathcal{P}$ garantit l'existence de l'ensemble X, et l'hypothèse d'induction en α implique que X n'est pas vide. Donc X a un plus petit élément, disons β. Mais cela signifie que $\mathcal{P}(\beta)$ est fausse, alors que $\mathcal{P}(\gamma)$ est vraie pour $\gamma < \beta$, contredisant l'hypothèse d'induction en β. La seule possibilité est donc qu'il n'existe pas d'ordinal α tel que $\mathcal{P}(\alpha)$ soit fausse. □

2.4. Borne supérieure; ordinaux limites.

▶ On montre que tout ensemble d'ordinaux possède une borne supérieure qui est un ordinal; on en déduit qu'il n'existe pas d'ensemble de tous les ordinaux. On introduit l'ordinal ω, et la notion d'ordinal limite. ◀

▷ *On a montré que l'intersection d'un ensemble d'ordinaux est un ordinal, plus petit élément de l'ensemble considéré. Quand on considère l'union, on a des résultats symétriques, à ceci près que l'ordinal obtenu est borne supérieure, mais pas forcément élément de l'ensemble, donc n'est pas forcément plus grand élément.* ◁

Proposition 2.16. (borne supérieure) *Tout ensemble d'ordinaux A possède une borne supérieure, à savoir $\bigcup A$.*

Démonstration. Posons $a = \bigcup A$. Par hypothèse, les éléments de A sont des ordinaux, donc sont transitifs, et le lemme 2.2(iii) entraîne que a est transitif. Ensuite, soient α, β, γ des éléments de a. Puisque α est un ordinal, on a $\alpha \notin \alpha$ par le lemme 2.4(ii). D'autre part, $\alpha \in \beta \in \gamma$ entraîne $\alpha \in \gamma$ puisque γ est un ordinal. Donc, la relation $\in\restriction_a$ est un ordre strict sur a.

Soit X une partie non vide de a. Posons $\alpha := \bigcap X$. Puisque X est un ensemble d'ordinaux, la proposition 2.13 garantit que α est un ordinal et que c'est le plus petit élément de X, c'est-à-dire qu'on a $\alpha \in \beta$ pour tout élément β de X distinct de α. C'est dire que $\in\restriction_a$ est un bon ordre et, par conséquent, a est un ordinal.

Pour tout α dans A, on a $\alpha \subseteq a$, soit $\alpha \leqslant a$, donc a est un majorant de A. Ensuite, supposons que β est un minorant strict de a. Cela signifie qu'on a $\beta < a$, soit $\beta \in \bigcup A$. Par définition de l'union, cela signifie qu'il existe α dans A tel qu'on ait $\beta \in \alpha$, donc $\beta < \alpha$, et β n'est pas un majorant de A. Par conséquent, a est le plus petit des majorants de A, c'est-à-dire qu'il en est borne supérieure. □

Une conséquence directe est que les ordinaux ne forment pas un ensemble :

[4] Comme pour la proposition 1.7, la restriction sur la propriété $\mathcal{P}$ tient au flou de la formulation ; tout ceci sera précisé dans le chapitre III.

PROPOSITION 2.17. (paradoxe de Burali–Forti) *Aucun ensemble ne contient tous les ordinaux.*

DÉMONSTRATION. Supposons qu'il existe un ensemble contenant tous les ordinaux. Alors, par séparation, il existe un ensemble Ω de tous les ordinaux. Par la proposition 2.16, $\bigcup\Omega$ est un ordinal, et on a $\alpha \leqslant \bigcup\Omega$ pour tout ordinal α dans Ω, donc pour tout ordinal α. En particulier, on a $\bigcup\Omega < S(\bigcup\Omega) \leqslant \bigcup\Omega$, d'où $\bigcup\Omega \in \bigcup\Omega$, contredisant le lemme 2.4(*ii*). □

L'application de la proposition 2.16 à la famille des ordinaux $\underline{n}$ mène à un nouvel ordinal :

DÉFINITION 2.18. (omega) On note ω la borne supérieure des ordinaux $\underline{n}$ pour n entier.

▷ *L'ordinal ω est le premier ordinal plus grand que tous les ordinaux finis. Par construction, il se trouve contenir tous les ordinaux $\underline{n}$, et est donc un ensemble infini ainsi qu'en témoigne l'injection non surjective $\underline{n} \mapsto \underline{n+1}$. Par conséquent, ω est le premier ordinal infini.*

Le point important pour la suite est que ω vient après tous les ordinaux finis, ce que Cantor exprimait par le qualificatif transfini. *Qu'en tant qu'ensemble, l'ordinal ω se trouve être infini résulte de la construction adoptée ici, mais c'est un point secondaire — même si, et c'est dommage, l'adjectif « infini » a pris le pas sur « transfini » dans l'usage.* ◁

LEMME 2.19. *La relation $\omega = \bigcup\omega$ est vérifiée.*

DÉMONSTRATION. Comme $k < n$ entraîne $\underline{k} \in \underline{n}$, les éléments des éléments de ω coïncident avec les éléments de ω. □

▷ *Le lemme 2.19 suggère d'étudier systématiquement l'ensemble $\bigcup\alpha$ quand α est un ordinal. Ceci mène à partitionner les ordinaux (non nuls) en deux familles complémentaires.* ◁

LEMME 2.20. *Pour tout ordinal α,*
- ou bien $\beta < \alpha$ entraîne $S(\beta) < \alpha$ pour tout β, et on a alors $\bigcup\alpha = \alpha$,
- ou bien il existe β tel qu'on ait $\alpha = S(\beta)$, et on a alors $\bigcup\alpha = \beta$.

DÉMONSTRATION. Soit α un ordinal quelconque. Par définition, α est un ensemble transitif, donc on a $\bigcup\alpha \subseteq \alpha$, soit, puisque $\bigcup\alpha$ est un ordinal par la proposition 2.16, $\bigcup\alpha \leqslant \alpha$. Par ailleurs, par la proposition 2.12(*iii*), $\beta < \alpha$ entraîne $S(\beta) \leqslant \alpha$. Deux cas sont possibles : ou bien on a $S(\beta) < \alpha$ pour tout $\beta < \alpha$, ou bien il existe $\beta < \alpha$ vérifiant $S(\beta) \geqslant \alpha$, auquel cas on a nécessairement $S(\beta) = \alpha$.

Dans le premier cas, $\beta < \alpha$ entraîne $\beta < S(\beta) < \alpha$, soit $\beta \in S(\beta) \in \alpha$, et donc $\beta \in \bigcup\alpha$. Par conséquent, on a $\alpha \subseteq \bigcup\alpha$, et donc $\bigcup\alpha = \alpha$ d'après ce qui est au-dessus.

Dans le second cas, $\gamma < \beta$ entraîne $\gamma \in \beta \in \alpha$, donc $\gamma \in \bigcup\alpha$, d'où $\beta \subseteq \bigcup\alpha$. Inversement, par construction, on a $\bigcup\alpha = \bigcup(S(\beta)) = \bigcup\beta \cup \beta \subseteq \beta$, donc $\bigcup\alpha \subseteq \beta$, et, finalement, $\bigcup\alpha = \beta$. □

DÉFINITION 2.21. (successeur, limite) Un ordinal α est appelé *successeur* (*resp. limite*) s'il existe β vérifiant $\alpha = S(\beta)$ (*resp.* si α est distinct de $\underline{0}$ et vérifie $\alpha = \bigcup\alpha$).

EXEMPLE 2.22. Les ordinaux $\underline{1}$, $\underline{2}$, ... sont des ordinaux successeurs, tandis que ω est un ordinal limite, et c'est le plus petit ordinal limite. La suite des ordinaux continue ensuite avec de nouveaux ordinaux successeurs : $S(\omega)$, $S^2(\omega)$, *etc.* On peut donc raffiner un peu la représentation des ordinaux comme suggéré sur la figure 11.

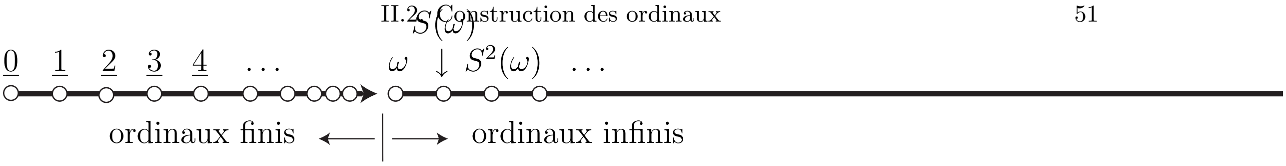


FIGURE 11. La suite des ordinaux (2) : l'ordinal ω n'est successeur d'aucun ordinal, mais c'est la limite des ordinaux plus petits ; comme la suite des ordinaux n'est pas un ensemble, il est naturel de l'imaginer très longue.

▷ *L'appellation d'ordinal limite provient de la topologie. Pour chaque ordre total sur un ensemble A, on introduit la topologie dont une base d'ouverts est la famille des intervalles ouverts* $]a, b[$. *La topologie de* $\mathbb{R}$ *s'obtient ainsi à partir de l'ordre des réels, de même que la topologie discrète sur* $\mathbb{Z}$ *puisque chaque singleton dans* $\mathbb{Z}$ *est un intervalle ouvert. Dans le cas des ordinaux, noter que chaque intervalle ouvert* $]\alpha, \beta[$ *coïncide avec l'intervalle semi-ouvert* $[S(\alpha), \beta[$. ◁

PROPOSITION 2.23. (topologie) *Un ordinal non nul est limite (resp. successeur) si et seulement si c'est un point d'accumulation (resp. un point isolé) pour la topologie de l'ordre.*

DÉMONSTRATION. Soient λ un ordinal limite, et U un ouvert contenant λ. Par définition, il existe un intervalle ouvert $]\alpha, \beta[$ inclus dans U et contenant λ. On a donc $\alpha < \lambda < \beta$. Alors $S(\alpha)$ est un autre point de cet intervalle, donc de U, ce qui montre que λ est point d'accumulation (à gauche). Inversement, supposons $\alpha = S(\beta)$. Alors on a $\{\alpha\} =]\beta, S(\alpha)[$, et α est donc un point isolé. □

La partition des ordinaux en $\underline{0}$, ordinaux successeurs et ordinaux limites permet de reformuler le principe d'induction dans des termes plus voisins de l'induction sur les entiers :

PROPOSITION 2.24. (induction II) *Soit* $\mathcal{P}(\alpha)$ *une propriété pour laquelle la séparation est valide. Supposons que*
- $\mathcal{P}(\underline{0})$ *est vraie;*
- *si* $\mathcal{P}(\alpha)$ *est vraie, alors* $\mathcal{P}(S(\alpha))$ *l'est aussi,*
- *si* λ *est limite et si* $\mathcal{P}(\alpha)$ *est vraie pour* $\alpha < \lambda$, *alors* $\mathcal{P}(\lambda)$ *est vraie.*

Alors $\mathcal{P}(\alpha)$ *est vraie pour tout ordinal* α.

DÉMONSTRATION. Comme pour la proposition 2.15, si $\mathcal{P}(\alpha)$ n'était pas vraie pour tout α, il existerait un plus petit élément α tel que $\mathcal{P}(\alpha)$ soit fausse, et les trois clauses de l'énoncé interdisent respectivement que α soit $\emptyset$, un ordinal successeur, et un ordinal limite. □

2.5. Le théorème de comparaison.

▶ On montre que tout ensemble bien ordonné est isomorphe à un unique ordinal. ◀

▷ *A chaque ordinal* α *est associé un bon ordre, à savoir* $\in\restriction_{\alpha}$. *Les ordinaux constituent donc une famille particulière d'ensembles bien ordonnés. Un des intérêts de cette construction est que cette famille fournit un représentant distingué et un seul pour chaque type de bon ordre.* ◁

PROPOSITION 2.25. (comparaison) *Tout ensemble bien ordonné est isomorphe à un unique ordinal.*

Démonstration. Essentiellement, le résultat est dans la proposition 1.18 : si $(A, <)$ est un ensemble bien ordonné, alors on le compare à la suite des ordinaux, et la proposition dit que ou bien $(A, <)$ est isomorphe à la suite des ordinaux entière, ou bien cette dernière est isomorphe à un segment initial de $(A, <)$, ou bien $(A, <)$ est isomorphe à un segment initial de la suite des ordinaux. Les deux premiers cas sont exclus car la suite des ordinaux n'est pas un ensemble, donc il ne reste que le troisième cas, et, comme un segment initial de la suite des ordinaux est un ordinal, on a le résultat escompté.

Comme la proposition 1.18 ne concerne que deux ensembles bien ordonnés, l'argument précédent peut paraître un peu rapide, et on peut le reprendre. Soit $(A, <)$ un ensemble bien ordonné quelconque. On considère la correspondance F de A vers les ordinaux définie par

$$F(a) = \alpha \text{ si et seulement si } I_<(a) \text{ est isomorphe à } (\alpha, \in).$$

Comme dans la section 1, F est fonctionnelle, c'est-à-dire qu'il existe au plus une valeur de α pour chaque valeur de a, et injective, c'est-à-dire qu'il existe au plus une valeur de a pour chaque valeur de α. Donc F établit un isomorphisme de son domaine sur son image.

Le même argument que dans la section 1 montre que le domaine de F est A ou un segment initial de $(A, <)$, et que l'image de F est la suite entière des ordinaux, ou un segment initial de celle-ci, et que le cas « segment initial + segment initial » est impossible. Comme aucun ensemble ne contient tous les ordinaux, le cas où l'image serait toute la suite des ordinaux est exclu [5], et le seul cas restant est celui où le domaine de F est A et où l'image de F est un segment initial de la suite des ordinaux, c'est-à-dire, par construction, un ordinal. On a donc ainsi un isomorphisme de $(A, <)$ sur un ordinal.

Celui-ci est unique, puisque, par le lemme 1.17, un bon ordre n'est jamais isomorphe à un de ses segments initiaux. □

3. Arithmétique ordinale

▶ On définit sur la collection des ordinaux trois opérations, la somme, le produit, et l'exponentiation, qui prolongent les opérations arithmétiques des nombres entiers. ◀

▷ *Comme chaque classe d'isomorphisme de bons ordres contient un unique ordinal, chaque opération sur les bons ordres induit immédiatement une opération similaire sur les ordinaux via une définition du type « $\alpha * \beta$ est l'unique ordinal isomorphe à... ». L'application du principe aux opérations de la section 1 mène naturellement aux opérations dites arithmétiques sur les ordinaux.*

L'un des intérêts immédiats de l'introduction des opérations arithmétiques sur les ordinaux est la possibilité de nommer *beaucoup plus d'ordinaux que ce qu'on a fait jusqu'à présent, et, de là, de rendre plus concrète la richesse de la suite des ordinaux.* ◁

3.1. Un critère.

▶ On donne un critère général permettant d'établir des inégalités entre ordinaux. ◀

▷ *Dans la suite, on affirmera souvent soit des égalités, soit des inégalités strictes ou larges entre des ordinaux, eux-mêmes introduits comme les uniques ordinaux isomorphes à divers ensembles bien ordonnés. La méthode de démonstration consiste dans la plupart des cas à appliquer le critère suivant. On le donne sous forme de conditions suffisantes en vue des utilisations ultérieures, mais on pourra noter que les conditions sont également néécessaires.* ◁

[5] cet argument de bon sens n'est pour le moment étayé par aucune démonstration véritable ; on y reviendra au chapitre III — comme du reste sur l'ensemble des démonstrations de ce chapitre

Lemme 3.1. *Supposons que α et β sont deux ordinaux respectivement isomorphes à des ensembles bien ordonnés $\mathcal{A}$ et $\mathcal{B}$.*
(i) Pour montrer $\alpha = \beta$, il suffit de construire une bijection strictement croissante de $\mathcal{A}$ sur $\mathcal{B}$.
(ii) Pour montrer $\alpha < \beta$, il suffit de construire une bijection strictement croissante de $\mathcal{A}$ sur un segment initial de $\mathcal{B}$.
(iii) Pour montrer $\alpha \leqslant \beta$, il suffit de construire une injection strictement croissante de $\mathcal{A}$ dans $\mathcal{B}$.

Démonstration. Le point (i) n'est qu'une reformulation de l'unicité dans la proposition 2.25. Pour (ii), l'existence d'un isomorphisme de $\mathcal{A}$ dans un segment initial de $\mathcal{B}$ entraîne celle d'un isomorphisme de $(\alpha, <)$ sur un segment initial de $(\beta, <)$. Or le segment initial de $(\beta, <)$ déterminé par un élément γ se trouve coïncider, en tant qu'ensemble, avec γ lui-même. Dire que $(\alpha, <)$ est isomorphe au segment initial de $(\beta, <)$ déterminé par γ équivaut donc à dire que α est égal à γ, et on a alors $\alpha = \gamma < \beta$.

Pour (iii), une injection croissante de $\mathcal{A}$ dans $\mathcal{B}$ fournit par transport une injection croissante, disons f, de $(\alpha, <)$ dans $(\beta, <)$. Si on avait $\beta < \alpha$, l'application f serait une injection croissante de $(\beta, <)$ dans un de ses segments initiaux, contredisant la démonstration du lemme 1.13. Donc $\beta < \alpha$ est faux, et, comme l'ordre des ordinaux est un ordre total, la seule possibilité est $\alpha \leqslant \beta$. □

▷ *On notera que l'existence d'une injection strictement croissante non surjective de $(\alpha, <)$ dans $(\beta, <)$ n'entraîne* pas *$\alpha < \beta$: par exemple, l'application $\alpha \mapsto S(\alpha)$ est une injection strictement croissante non surjective de $(\omega, <)$ dans lui-même, et pourtant on n'a pas $\omega < \omega$. On ne peut conclure à une inégalité stricte que dans le cas particulier où l'image de l'injection est un segment initial du second ordinal.* ◁

3.2. Addition ordinale.

► La première, et plus simple, opération est l'addition des ordinaux, calquée sur l'addition des bons ordres. ◄

▷ *L'addition ordinale ressemble à l'addition des entiers, dont elle est (à isomorphisme près) une extension, mais des différences importantes apparaissent dès qu'on considère les ordinaux infinis. En particulier, l'addition ordinale n'est pas commutative.* ◁

Définition 3.2. (addition) Pour α, β ordinaux, on définit $\alpha+\beta$ comme l'unique ordinal γ tel que $(\gamma, \in)$ soit isomorphe à $(\alpha, \in) + (\beta, \in)$.

Exemple 3.3. Pour n et k entiers, l'ordinal $\underline{n} + \underline{k}$ est un ordinal qui a $n + k$ éléments, il s'agit donc nécessairement de l'ordinal $\underline{n + k}$: l'application $n \mapsto \underline{n}$ est un homomorphisme injectif de $(\mathbb{N}, +)$ dans les ordinaux munis de l'addition. Donc, en considérant que l'ordinal $\underline{n}$ est une copie de l'entier n, on peut dire que l'addition ordinale prolonge l'addition des entiers.

Calculons maintenant $\underline{1} + \omega$. Il s'agit de déterminer l'unique ordinal γ tel que l'ordre-somme $(\underline{1}, \in) + (\omega, \in)$ soit isomorphe à $(\gamma, \in)$. Or définissons $f : \underline{1} \uplus \omega \to \omega$ par $f((\underline{0}, 1)) = \underline{0}$ et $f((\theta, 2) = S(\theta)$ pour $\theta \in \omega$. L'application f est injective, puisque S l'est, et surjective puisque, par construction, tout élément de ω est soit $\underline{0}$, soit le successeur d'un élément de ω. Donc f est une bijection. De plus, f

est strictement croissante puisque $f((\underline{0}, 1))$ vient avant tout élément de la forme $f((\theta, 2))$. Par le lemme 3.1(i), on déduit l'égalité $\underline{1} + \omega = \omega$. Cette égalité montre que l'addition des ordinaux n'est *pas* commutative: on a $\underline{1}+\omega = \omega \neq S(\omega) = \omega+\underline{1}$. De même, elle montre que l'addition des ordinaux n'admet pas la simplification à droite: on a $\underline{1} + \omega = \underline{0} + \omega$, et pourtant on n'a pas $\underline{1} = \underline{0}$.

Proposition 3.4. (addition) (i) *On a toujours* $\alpha + \underline{0} = \underline{0} + \alpha = \alpha$.
(ii) *On a toujours* $\alpha + \underline{1} = S(\alpha)$. *On a* $\underline{1} + \alpha = S(\alpha)$ *pour* α *fini, et* $\underline{1} + \alpha = \alpha$ *pour* α *infini.*
(iii) *L'addition ordinale est associative: on a toujours* $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Démonstration. (i) L'application f définie par $f((\theta, 1)) = \theta$ est une bijection de $A \uplus \emptyset$ sur A, et elle est croissante vis-à-vis de l'ordre somme de $(A, <)$ et $(\emptyset, \in)$. Par le lemme 3.1(i), on déduit $\alpha + \underline{0} = \alpha$. L'argument est similaire pour $\underline{0} + \alpha$.

(ii) L'application f définie par $f((\theta, 1)) = \theta$ pour $\theta \in \alpha$, et $f((\underline{0}, 2)) = \alpha$ définit une bijection de $\alpha \uplus \{\underline{0}\}$, c'est-à-dire de $\alpha \uplus \underline{1}$, sur $S(\alpha)$. Cette bijection est croissante de $(\alpha, <) + (\underline{1}, <)$ dans $(S(\alpha), <)$, car, dans $(\alpha, <) + (\underline{1}, <)$, l'élément $(\underline{0}, 2)$ est placé après tous les éléments $(\theta, 1)$, de même que, dans $(S(\alpha), <)$, l'élément α est placé après tous les éléments θ de α. Toujours par le critère du lemme 3.1(i), on déduit $\alpha + \underline{1} = S(\alpha)$.

Une construction symétrique définissant f de $\underline{1} \uplus \alpha$ dans $S(\alpha)$ par $f((\underline{0}, 1)) = \underline{0}$ et $f((\theta, 2) = S(\theta)$ pour $\theta \in \alpha$ fournit une injection croissante de $(\underline{1}, <) + (\alpha, <)$ dans $(S(\alpha), <)$, mais rien ne permet d'affirmer la surjectivité en général: le lemme 3.1(iii) donne seulement $\underline{1}+\alpha \leqslant S(\alpha)$. On distingue deux cas. Supposons d'abord $\alpha < \omega$, c'est-à-dire α fini. Alors f est surjective, et on déduit $\underline{1}+\alpha = S(\alpha)$. En effet, l'image de f consiste en $\underline{0}$ et en tous les ordinaux $S(\theta)$ pour $\theta \in \alpha$, c'est-à-dire en $\underline{0}$ et en tous les ordinaux successeurs plus petits que $S(\alpha)$: comme α, et $S(\alpha)$, sont finis, tous les ordinaux plus petits que $S(\alpha)$ et distincts de $\underline{0}$ sont successeurs. Supposons maintenant $\alpha \geqslant \omega$. Alors ω n'appartient pas à l'image de f. Définissons $g : \{\underline{0}\} \uplus \alpha \to \alpha$ par $g((\underline{0}, 1)) = \underline{0}$, $g((\theta, 2)) = S(\theta)$ pour $\theta \in \omega$, et $g((\theta, 2)) = \theta$ pour $\theta \in \alpha$ avec $\theta \geqslant \omega$. Alors g est une bijection croissante, impliquant $\underline{1} + \alpha = \alpha$.

(iii) Il suffit de montrer que $((\alpha, \in) + (\beta, \in)) + (\gamma, \in)$ et $(\alpha, \in) + ((\beta, \in) + (\gamma, \in))$ sont isomorphes, ce qui résulte de la proposition 1.22. □

Les liens entre l'addition et l'ordre des ordinaux étendent eux aussi ceux qui existent dans le cas des entiers, à ceci près qu'il faut distinguer entre addition à gauche et addition à droite.

Lemme 3.5. *Pour* α, β *ordinaux,* $\alpha < \beta$ *est vraie si et seulement il existe* δ *non nul vérifiant* $\alpha + \delta = \beta$.

Démonstration. Par construction, $(\alpha, \in)$ est un segment initial de $(\alpha, \in) + (\delta, \in)$, donc $\alpha + \delta = \beta$ entraîne $\alpha \leqslant \beta$. Inversement, supposons $\alpha \leqslant \beta$. Alors $(\beta \setminus \alpha, \in)$ est un ensemble bien ordonné, donc il est isomorphe à un ordinal δ. Par construction, $(\alpha, \in)$ est le segment initial de $(\beta, \in)$ déterminé par α, c'est-à-dire qu'on a $\alpha = \{\gamma \in \beta\,;\, \gamma < \alpha\}$. Donc, dans l'ordre sur β, tous les éléments de $\beta \setminus \alpha$ sont après tous les éléments de α, ce qui est dire qu'on a $(\beta, \in) \cong (\alpha, \in) + (\beta \setminus \alpha, \in)$, d'où l'égalité $\alpha + \delta = \beta$. □

Proposition 3.6. (addition et ordre) (i) *Pour chaque ordinal* α*, l'addition de* α *à gauche est une opération strictement croissante et continue:* $\beta < \beta'$ *entraîne* $\alpha + \beta < \alpha + \beta'$*, et, pour* λ *limite, on a* $\alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta)$.

(ii) Pour chaque ordinal β, l'addition de β à droite est une opération non décroissante et semi-continue inférieurement : $\alpha \leqslant \alpha'$ entraîne $\alpha + \beta \leqslant \alpha' + \beta$, et, pour λ limite, on a $\lambda + \beta \geqslant \sup_{\alpha<\lambda}(\alpha + \beta)$.

Démonstration. (i) Supposons $\beta < \beta'$. L'application f définie par $f((\theta, 1)) = (\theta, 1)$ pour θ dans α et $f((\theta, 2)) = (\theta, 2)$ pour θ dans β est une injection strictement croissante de $(\alpha, <) + (\beta, <)$ sur le segment initial de $(\alpha, <) + (\beta', <)$ déterminé par $\alpha + \beta$. Par le lemme 3.1(ii), on déduit $\alpha + \beta < \alpha + \beta'$.

Supposons λ limite. D'après ce qui précède, $\beta < \lambda$ entraîne $\alpha + \beta < \alpha + \lambda$, donc, en passant à la borne supérieure, on a $\sup_{\beta<\lambda}(\alpha + \beta) \leqslant \alpha + \lambda$. Inversement, soit $\theta < \alpha + \lambda$. Alors ou bien on a $\theta < \alpha$, ou bien, par le lemme 3.5, il existe δ vérifiant $\theta = \alpha + \delta$. Dans ce cas, $\theta < \alpha + \lambda$ entraîne $\delta < \lambda$: il existe donc β plus petit que λ, à savoir $\beta = \delta$, tel qu'on ait $\theta \leqslant \alpha + \beta$, et on a donc $\alpha + \lambda \leqslant \sup_{\beta<\lambda}(\alpha + \beta)$.

(ii) Supposons $\alpha \leqslant \alpha'$. L'application g définie par $g((\theta, 1)) = (\theta, 1)$ pour θ dans α et $f((\theta, 2)) = (\theta, 2)$ pour θ dans β est une injection strictement croissante de $(\alpha, <) + (\beta, <)$ dans $(\alpha', <) + (\beta, <)$. Par le lemme 3.1$(iii)$, on déduit $\alpha + \beta \leqslant \alpha' + \beta$. Supposons enfin λ limite. D'après ce qui précède, $\alpha < \lambda$ entraîne $\lambda + \beta \geqslant \alpha + \beta$, d'où $\lambda + \beta \geqslant \sup_{\alpha<\lambda}(\alpha + \beta)$. □

D'après (i), l'addition ordinale admet la simplification à gauche : $\alpha+\beta = \alpha+\beta'$ entraîne $\beta = \beta'$, et, de là, l'ordinal δ du lemme 3.5 est unique[6]. Les résultats du point (ii) sont optimaux : on a $\underline{0} < \underline{1}$ mais $\underline{0} + \omega = \underline{1} + \omega$, donc $\alpha < \alpha'$ n'entraîne pas $\alpha + \beta < \alpha' + \beta$; de même, on a $\omega + \underline{1} > \sup_{\alpha<\omega}(\alpha + \underline{1}) = \omega$, donc, pour λ limite, $\lambda + \beta$ n'est pas nécessairement égal à $\sup_{\alpha<\lambda}(\alpha + \beta)$.

La proposition 3.6 mène à une caractérisation récursive de l'addition ordinale, ou plus exactement des translations à gauche associées.

Corollaire 3.7. *Pour tout ordinal α, la translation à gauche pour l'addition de α, c'est-à-dire l'application $\theta \mapsto \alpha + \theta$, est déterminée par les relations*

$$(3.1) \qquad \alpha + \underline{0} = \alpha, \ \alpha + S(\beta) = S(\alpha + \beta), \ \alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta) \text{ pour } \lambda \text{ limite.}$$

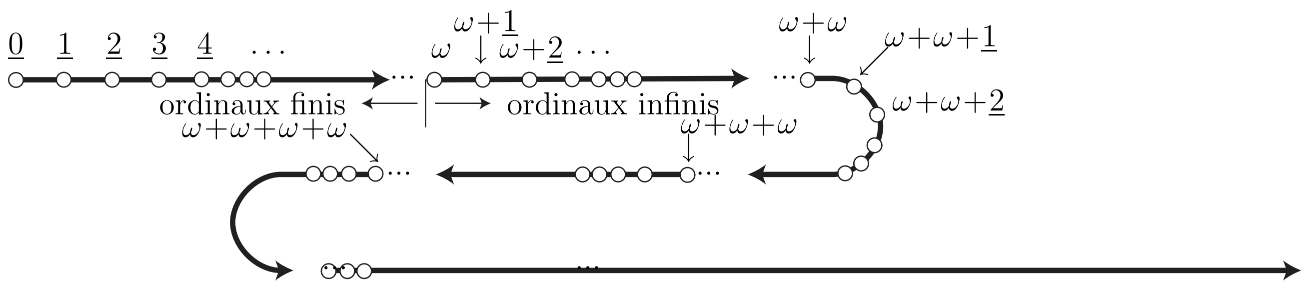


Figure 12. La suite des ordinaux (3) : l'opération $\theta \mapsto \theta + \omega$ permet de faire des sauts de taille ω inaccessibles à l'opération successeur, par exemple $\omega + \omega$ ou $\omega + \omega + \omega$

[6]Cet ordinal pourrait être noté $\beta - \alpha$, mais ce serait une option maladroite car, dans un contexte non commutatif, α devrait plutôt figurer à gauche de β.

3.3. Multiplication ordinale.

▶ La seconde opération est le produit. La multiplication ordinale prolonge celle des entiers, mais, comme dans le cas de l'addition, des différences apparaissent avec les ordinaux infinis, et, en particulier, la multiplication ordinale n'est ni commutative, ni distributive à droite par rapport à l'addition. Par contre la division euclidienne se prolonge. ◀

DÉFINITION 3.8. (multiplication) Pour α, β ordinaux, on définit $\alpha \cdot \beta$ comme l'unique ordinal γ tel que $(\gamma, \in)$ soit isomorphe à $(\alpha, \in) \times (\beta, \in)$.

EXEMPLE 3.9. (multiplication) Pour n et k entiers, l'ordinal $\underline{n}\cdot\underline{k}$ est un ordinal qui a nk éléments, il s'agit donc nécessairement de l'ordinal $\underline{nk}$: l'application $n \mapsto \underline{n}$ est un homomorphisme injectif de $(\mathbb{N}, \times)$ dans les ordinaux munis du produit. A l'identification de $\underline{n}$ avec n près, la multiplication ordinale prolonge celle des entiers naturels.

Comme autre exemple, calculons $\underline{2} \cdot \omega$. Il s'agit de ω copies de $\underline{2}$, c'est-à-dire de $\{\underline{0}, \underline{1}\}$, placées bout à bout. Définissons $f : \{\underline{0}, \underline{1}\} \times \omega \to \omega$ par $f((\underline{0}, \theta)) = \theta + \theta$ et $f((\underline{1}, \theta)) = \theta + \theta + \underline{1}$. Alors f est une bijection strictement croissante de $(\underline{2}, <) \times (\omega, <)$ sur $(\omega, <)$. On a donc $\underline{2} \cdot \omega = \omega$.

PROPOSITION 3.10. (multiplication) (i) *On a toujours* $\alpha \cdot \underline{0} = \underline{0} \cdot \alpha = \underline{0}$, *et* $\underline{1} \cdot \alpha = \alpha \cdot \underline{1} = \alpha$.
(ii) *La multiplication ordinale est associative et distributive à gauche par rapport à l'addition : on a toujours* $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ *et* $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

DÉMONSTRATION. (i) Comme les produits cartésiens $\alpha \times \emptyset$ et $\emptyset \times \alpha$ sont vides, les deux premières égalités sont claires. Ensuite, les applications définies par $\theta \mapsto (\theta, \underline{0})$ et $\theta \mapsto (\underline{0}, \theta)$ établissent une bijection de α sur $\alpha \times \{\underline{0}\}$ et $\{\underline{0}\} \times \alpha$ respectivement. Ces bijections sont strictement croissantes, et on obtient les deux dernières égalités.

Le point (ii) est une application directe de la proposition 1.26 sur l'addition et la multiplication des ordres. □

Comme on a $\underline{2} = \underline{1} + \underline{1}$, la distributivité de la multiplication entraîne $\alpha \cdot \underline{2} = \alpha + \alpha$ pour tout ordinal α et, inductivement, $\alpha \cdot \underline{n} = \alpha + \cdots + \alpha$, n fois α, pour tout entier n. En particulier, on a $\omega \cdot \underline{2} = \omega + \omega$. Par contre, on a vu qu'on a $\underline{2} \cdot \omega = \omega$. Donc la multiplication ordinale n'est pas commutative ; puisqu'on a

$$(\underline{1} + \underline{1}) \cdot \omega = \underline{2} \cdot \omega = \omega \neq \omega + \omega = \underline{1} \cdot \omega + \underline{1} \cdot \omega,$$

et donc la multiplication ordinale n'est pas non plus distributive à droite par rapport à l'addition.

▷ *Le résultat technique suivant est une première étape en direction de la division euclidienne. Il sera précisé plus loin, mais permet d'établir facilement la compatibilité de la multiplication ordinale avec l'ordre des ordinaux.* ◁

LEMME 3.11. *Pour tout ordinal* γ *vérifiant* $\gamma < \alpha \cdot \beta$, *il existe un couple d'ordinaux* (ρ, σ) *avec* $\rho < \alpha$ *et* $\sigma < \beta$ *vérifiant* $\gamma = \alpha \cdot \sigma + \rho$.

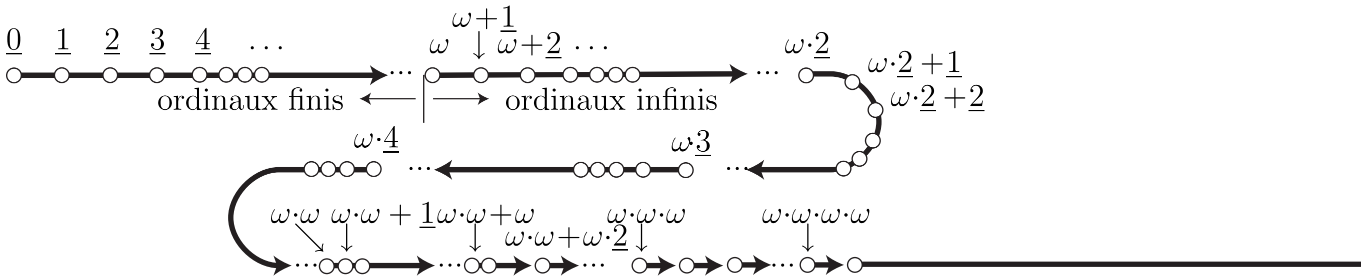


FIGURE 13. La suite des ordinaux (4) : grâce à la multiplication ordinale, on peut enrichir à nouveau le schéma. Noter qu'on a $\omega \cdot \underline{2} = \omega + \omega$, $\omega \cdot \underline{3} = \omega + \omega + \omega$, *etc.* L'opération $\theta \mapsto \theta \cdot \omega$ permet de faire des sauts encore plus grands, et d'atteindre des ordinaux inaccessibles à l'addition comme $\omega \cdot \omega$ ou $\omega \cdot \omega \cdot \omega$.

DÉMONSTRATION. Le résultat étant vide pour $\alpha = \underline{0}$, on suppose $\alpha > \underline{0}$. Par définition, il existe un isomorphisme f de $(\alpha, \in) \times (\beta, \in)$ sur $(\alpha \cdot \beta, \in)$. Soit γ un ordinal plus petit que $\alpha \cdot \beta$, donc, par construction, un élément de $\alpha \cdot \beta$. Posons $(\rho, \sigma) = f^{-1}(\gamma)$. Par construction, on a $\rho < \alpha$ et $\sigma < \beta$. Toujours par construction, $(\gamma, \in)$ est le segment initial de $(\alpha \cdot \beta, \in)$ déterminé pae γ, et il est donc isomorphe au segment initial de $(\alpha, \in) \times (\beta, \in)$ déterminé par (ρ, σ). Par définition de l'ordre produit, ce segment initial consiste en les couples (ξ, η) vérifiant $\xi < \alpha$ et $\eta < \sigma$, suivis par les couples (η, σ) vérifiant $\eta < \rho$. Il est donc isomorphe à l'ordinal $\alpha \cdot \sigma + \rho$, et on a donc $\gamma = \alpha \cdot \sigma + \rho$. □

PROPOSITION 3.12. (multiplication et ordre) (i) *Pour chaque ordinal α distinct de $\underline{0}$, la multiplication par α à gauche est une opération strictement croissante et continue : $\beta < \beta'$ entraîne $\alpha \cdot \beta < \alpha \cdot \beta'$, et, pour λ limite, on a $\alpha \cdot \lambda = \sup_{\beta<\lambda} \alpha \cdot \beta$.*
(ii) *Pour chaque ordinal β, la multiplication par β à droite est une opération non décroissante et semi-continue inférieurement : $\alpha \leqslant \alpha'$ entraîne $\alpha \cdot \beta \leqslant \alpha' \cdot \beta$, et, pour λ limite, on a $\lambda \cdot \beta \geqslant \sup_{\alpha<\lambda} \alpha \cdot \beta$.*

DÉMONSTRATION. (i) Supposons $\alpha \geqslant \underline{1}$ et $\beta < \beta'$. L'application identité sur $\alpha \times \beta$ définit un isomorphisme de $(\alpha, <) \times (\beta, <)$ sur le segment initial de $(\alpha, <) \times (\beta', <)$ déterminé par $(\underline{0}, \beta)$. Par le lemme 3.1(ii), on en déduit $\alpha \cdot \beta < \alpha \cdot \beta'$.

Supposons λ limite. Le résultat précédent entraîne $\alpha \cdot \lambda \geqslant \sup_{\beta<\lambda} \alpha \cdot \beta$. Inversement, supposons $\theta < \alpha \cdot \lambda$. Par le lemme 3.11, il existe un couple (ρ, σ) dans $\alpha \times \lambda$ vérifiant $\theta = \alpha \cdot \sigma + \rho$. On a donc

$$\theta = \alpha \cdot \sigma + \rho < \alpha \cdot \sigma + \alpha = \alpha \cdot \sigma + \alpha \cdot \underline{1} = \alpha \cdot (\sigma + \underline{1}) = \alpha \cdot S(\sigma),$$

ce qui montre qu'il existe β plus petit que λ, à savoir $\beta = S(\sigma)$, vérifiant $\theta \leqslant \alpha \cdot \beta$. On a donc $\alpha \cdot \lambda \leqslant \sup_{\beta<\lambda} \alpha \cdot \beta$.

(ii) Supposons $\alpha \leqslant \alpha'$. L'application identité sur $\alpha \times \beta$ définit une injection strictement croissante de $((\alpha, <) \times (\beta, <))$ dans $(\alpha', <) \times (\beta, <)$. Par le lemme 3.1$(iii)$, on en déduit $\alpha \cdot \beta \leqslant \alpha' \cdot \beta$. Pour λ limite, on déduit $\alpha \cdot \lambda \geqslant \sup_{\beta<\lambda} \alpha \cdot \beta$. □

Une conséquence du point (i) est que la multiplication ordinale restreinte aux ordinaux non nuls admet la simplification à gauche : $\alpha \cdot \beta = \alpha \cdot \beta'$ entraîne $\beta = \beta'$ pour $\alpha \neq \underline{0}$. Comme dans le cas de l'addition, le point (ii) est optimal : on a $\underline{0} < \underline{1} < \underline{2}$ et $\underline{1} \cdot \omega = \underline{2} \cdot \omega = \omega$, donc $\underline{0} < \alpha < \alpha'$ n'entraîne pas $\alpha \cdot \beta < \alpha' \cdot \beta$ en général ; de même, on a $\omega \cdot \underline{2} > \sup_{n<\omega} n \cdot \underline{2} = \omega$, ce qui montre qye, pour λ limite, $\lambda \cdot \beta$ n'est pas nécessairement égal à $\sup_{\alpha<\lambda} \alpha \cdot \beta$.

Une application de la proposition 3.12 est une caractérisation récursive des translations à gauche associées à la multiplication ordinale.

Corollaire 3.13. *Pour tout ordinal α, la translation à gauche pour la multiplication par α, c'est-à-dire l'application $x \mapsto \alpha \cdot x$, est déterminée par les relations*

$$\alpha \cdot \underline{0} = \underline{0}, \quad \alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha, \quad \alpha \cdot \lambda = \sup_{\beta<\lambda}(\alpha \cdot \beta) \text{ pour } \lambda \text{ limite.} \tag{3.2}$$

On peut alors établir l'unicité des ordinaux mis en jeu dans le lemme 3.11, et déduire l'énoncé optimal pour la division euclidienne des ordinaux, analogue complet à la division euclidienne des entiers :

Proposition 3.14. (division) *Pour tout ordinal β, et tout ordinal non nul α, il existe un unique couple d'ordinaux (ρ, σ) vérifiant $\beta = \alpha \cdot \sigma + \rho$ avec $\rho < \alpha$; on a de plus $\sigma \leqslant \beta$.*

Démonstration. Par la proposition 3.12(*ii*), $\underline{1} \leqslant \alpha$ implique $\beta = \underline{1} \cdot \beta \leqslant \alpha \cdot \beta < \alpha \cdot S(\beta)$. Appliquant le lemme 3.11, on obtient l'existence de (ρ, σ) vérifiant $\beta = \alpha \cdot \sigma + \rho$ avec $\rho < \alpha$. On obtient de plus $\sigma \leqslant \alpha \cdot \sigma \leqslant \alpha \cdot \sigma + \rho = \beta$, donc nécessairement $\sigma \leqslant \beta$.

Reste à montrer l'unicité. Considérons deux ordinaux $\alpha \cdot \sigma + \rho$ et $\alpha \cdot \sigma' + \rho'$ avec $\rho, \rho' < \alpha$. Supposons $\sigma < \sigma'$, donc $\sigma + \underline{1} \leqslant \sigma'$. On déduit des propositions 3.6 et 3.12

$$\alpha \cdot \sigma + \rho < \alpha \cdot \sigma + \alpha = \alpha \cdot (\sigma + \underline{1}) \leqslant \alpha \cdot \sigma' \leqslant \alpha \cdot \sigma' + \rho',$$

donc $\alpha \cdot \sigma + \rho \neq \alpha \cdot \sigma' + \rho'$. L'argument est symétrique pour $\sigma > \sigma'$. Donc $\alpha \cdot \sigma + \rho = \alpha \cdot \sigma' + \rho'$ entraîne $\sigma = \sigma'$, donc $\alpha \cdot \sigma = \alpha \cdot \sigma'$, et de là $\rho = \rho'$ puisque l'addition ordinale admet la simplification à gauche.. □

Noter que, dans la division ordinale, le quotient σ n'est pas nécessairement plus petit que le dividende β : la division de ω par $\underline{2}$ est $\omega = \underline{2} \cdot \omega + \underline{0}$, avec un quotient ω égal au dividende, et un reste nul.

3.4. Exponentiation ordinale.

▶ La dernière opération arithmétique est l'exponentiation. ◀

Définition 3.15. (exponentiation) Pour α, β ordinaux, on définit α^β comme l'unique ordinal γ tel que $(\gamma, \in)$ soit isomorphe à $(\alpha, \in)^{(\beta, \in)}$.

Exemple 3.16. (exponentiation) Pour n, k entiers, $\underline{k}$ est un ensemble fini, et $\underline{n}^{(\underline{k})}$ est l'ensemble de toutes les applications de $\underline{k}$ dans $\underline{n}$, est a donc n^k éléments. On a donc nécessairement $\underline{n}^{\underline{k}} = \underline{n^k}$: l'exponentiation ordinale prolonge l'exponentiation des entiers.

Calculons $\underline{2}^\omega$. Il s'agit de déterminer l'ordinal isomorphe à $(\{\underline{0}, \underline{1}\}, <)^{(\omega, <)}$. Le domaine est ici l'ensemble des fonctions de ω dans $\{\underline{0}, \underline{1}\}$ à support fini, c'est-à-dire valant $\underline{1}$ pour un nombre fini de valeurs, et l'ordre est l'ordre lexicographique inverse. Par construction, la fonction constante $c_{\underline{0}}$ de valeur $\underline{0}$ est le plus élément.

Si f, g sont distinctes de $c_{\underline{0}}$, et si, avec les notations de la démonstration de la proposition 1.29, on a $s_1(f) < s_1(g)$, c'est-à-dire si le plus grand élément du support de f est plus petit que le plus petit élément du support de g, alors on a $f < g$ par définition. Pour chaque élément $\underline{n}$ de ω, le nombre de fonctions f de ω dans $\{\underline{0}, \underline{1}\}$ vérifiant $s_1(f) = \underline{n}$ est égal à 2^n. Il en résulte, classées par ordre croissant, les fonctions de ω dans $\{\underline{0}, \underline{1}\}$ à support fini sont d'abord $c_{\underline{0}}$, puis l'unique fonction dont le s_1 vaut $\underline{0}$, puis les 2 fonctions dont le s_1 vaut $\underline{1}$, puis les 4 fonctions dont le s_1 vaut $\underline{2}$, les 8 fonctions dont le s_1 vaut $\underline{3}$ *etc.* L'ordre ainsi obtenu est celui de ω, et on a donc la valeur $\underline{2}^{\omega} = \omega$.

Proposition 3.17. (exponentiation) (i) *On a toujours* $\alpha^{\underline{0}} = \underline{1}$, $\alpha^{\underline{1}} = \alpha$, *et* $\underline{1}^{\beta} = \underline{1}$; *pour* $\beta \neq \underline{0}$, *on a* $\underline{0}^{\beta} = \underline{0}$.
(ii) *On a toujours* $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$ *et* $\alpha^{\beta\cdot\gamma} = (\alpha^{\beta})^{\gamma}$.

Démonstration. (i) Il existe une seule application (à support fini) de $\emptyset$ dans α, à savoir l'application vide. L'ensemble $\alpha^{(\underline{0})}$ est un singleton, et donc $(\alpha^{(\underline{0})}, \in)$ est isomorphe à $(\underline{1}, \in)$. L'application $f \mapsto f(\underline{0})$ établit une bijection de $\alpha^{(\underline{1})}$ sur α, et, par définition des ordres, elle est strictement croissante, d'où $\alpha^{\underline{1}} = \alpha$. Ensuite, il existe une seule application (à support fini) de β dans $\underline{1}$, à savoir l'application constante de valeur $\underline{0}$. On a donc toujours $\underline{1}^{\beta} = \underline{1}$, puisque $\underline{1}$ est le seul ordinal à un élément. Enfin, si β n'est pas vide, il n'existe aucune application de β vers l'ensemble vide, donc on doit avoir $\underline{0}^{\beta} = \underline{0}$.

Le point (ii) est conséquence directe de la proposition 1.30. □

Partant de (ii), une induction donne pour tout entier n l'égalité $\alpha^{\underline{n}} = \alpha \cdot \ldots \cdot \alpha$, avec n fois α. Comme dans le cas de l'addition et de la multiplication ordinales, on étudie le comportement de l'exponentiation vis-à-vis de l'ordre.

Proposition 3.18. (exponentiation et ordre) (i) *Pour chaque ordinal* α *distinct de* $\underline{0}$ *et* $\underline{1}$, *l'exponentiation de base* α *est une opération strictement croissante et continue :* $\beta < \beta'$ *entraîne* $\alpha^{\beta} < \alpha^{\beta'}$, *et, pour* λ *limite, on a* $\alpha^{\lambda} = \sup_{\beta<\lambda} \alpha^{\beta}$.
(ii) *Pour chaque ordinal* β, *l'exponentiation d'exposant* β *est une opération non décroissante et semi-continue inférieurement :* $\alpha \leqslant \alpha'$ *entraîne* $\alpha^{\beta} \leqslant \alpha'^{\beta}$, *et, pour* λ *limite, on a* $\lambda^{\beta} \geqslant \sup_{\alpha<\lambda} \alpha^{\beta}$.

Démonstration. (i) Supposons $\alpha \geqslant \underline{2}$ et $\beta < \beta'$. L'application F définie par $F(f) = f\restriction_{\beta}$ définit un isomorphisme de $(\alpha, <)^{(\beta,<)}$ sur le segment initial de $(\alpha, <)^{(\beta',<)}$ déterminé par la fonction valant $\underline{1}$ en β et $\underline{0}$ partout ailleurs. Par le lemme 3.1(ii), on déduit $\alpha^{\beta} < \alpha^{\beta'}$.

Supposons λ limite. Par ce qui précède, $\beta < \lambda$ entraîne $\alpha^{\beta} < \alpha^{\lambda}$, donc on a $\alpha^{\lambda} \geqslant \sup_{\beta<\lambda} \alpha^{\beta}$. Inversement, supposons $\theta < \alpha^{\lambda}$. Il s'agit de montrer qu'il existe $\beta < \lambda$ tel qu'on ait $\theta < \alpha^{\beta}$, c'est-à-dire encore que, pour toute fonction à support fini f de λ dans α, le segment initial de $\alpha^{(\lambda)}$ déterminé par f peut être plongé dans un segment initial d'un ordinal α^{β} avec $\beta < \lambda$. Or, soit f une telle fonction. Le plus grand élément du support de f est un élément de λ, et, comme λ est limite, il existe β vérifiant $\beta < \lambda$ et tel que tout élément du support de f soit plus petit que β. L'application qui à toute fonction de λ dans α plus petite que f associe sa restriction à β est injective, car toute telle fonction a un support inclus dans β. On obtient ainsi un isomorphisme entre le segment initial déterminé par f et un segment initial d'un ordinal α^{β} avec $\beta < \lambda$, comme souhaité.

(ii) Supposons $\alpha \leqslant \alpha'$. L'application identité de $\alpha^{(\beta)}$ dans $\alpha'^{(\beta)}$ définit une injection croissante de $(\alpha, <)^{(\beta,<)}$ dans $(\alpha', <)^{(\beta,<)}$, et on déduit $\alpha^\beta \leqslant \alpha'^\beta$ par le lemme 3.1(iii). □

Le point (i) entraîne que l'exponentielle de base $\underline{2}$ au moins est injective : pour $\alpha \geqslant \underline{2}$, la relation $\alpha^\beta = \alpha^{\beta'}$ entraîne $\beta = \beta'$. Les résultats de (ii) sont optimaux : on a $\underline{2} < \underline{4}$ et $\underline{4}^\omega = (\underline{2}^{\underline{2}})^\omega = \underline{2}^{\underline{2}\cdot\omega} = \underline{2}^\omega$ (et la valeur commune est ω), donc $\alpha < \alpha'$ n'entraîne pas $\alpha^\beta < \alpha'^\beta$ en général. De même, on a $\omega^\omega > \omega^\beta$ pour tout ordinal fini β, donc en particulier $\omega^\omega > \omega$, alors qu'on a $\sup_{\alpha<\omega} \alpha^\omega = \omega$.

Corollaire 3.19. *Pour tout ordinal α, la translation à gauche $x \mapsto \alpha^x$ est déterminée par les relations*

$$\alpha^{\underline{0}} = \underline{1}, \quad \alpha^{S(\beta)} = \alpha^\beta \cdot \alpha, \quad \alpha^\lambda = \sup_{\beta<\lambda}(\alpha^\beta) \text{ pour } \lambda \text{ limite.} \tag{3.3}$$

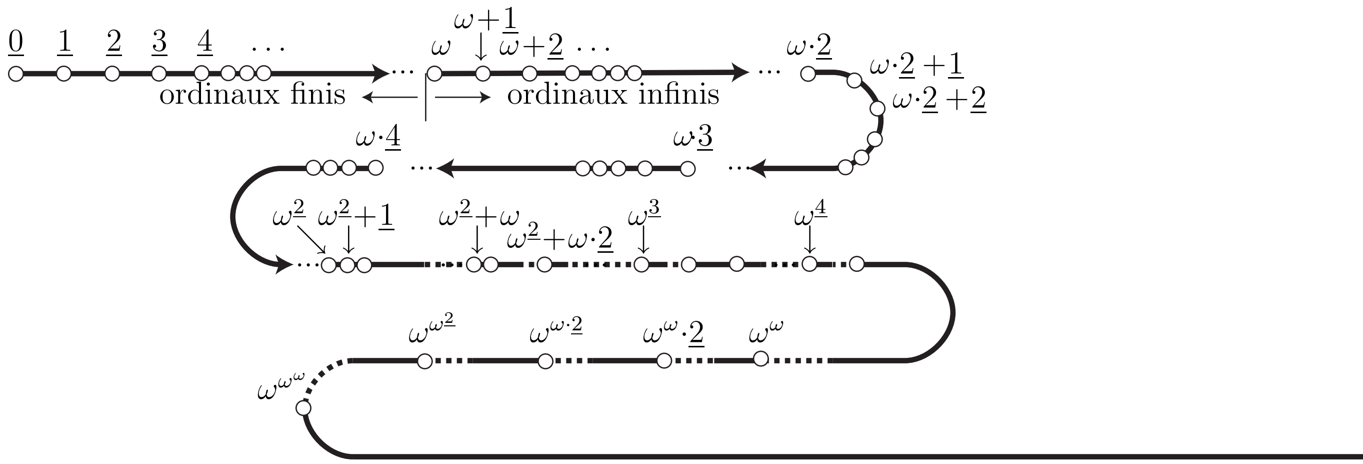


Figure 14. La suite des ordinaux (5) : grâce à l'exponentiation, on peut allonger une nouvelle fois le schéma. On a $\omega^{\underline{2}} = \omega\cdot\omega$, $\omega^{\underline{3}} = \omega\cdot\omega\cdot\omega$, *etc.* L'opération $\theta \mapsto \theta^\omega$ permet d'atteindre des ordinaux inaccessibles à l'addition et à la multiplication, comme ω^ω ou ω^{ω^ω}.

3.5. Ordinaux non dénombrables.

► On montre l'existence d'un ordinal non dénombrable et, plus généralement, l'existence pour chaque ordinal α d'un ordinal β ne s'injectant pas dans α. ◄

▷ *Les opérations arithmétiques ordinales permettent de spécifier des ordinaux transfinis de plus en plus grands, par exemple ω, ω^ω, ω^{ω^ω}, etc. L'opération de passage à la borne supérieure permet d'aller plus loin, par exemple en introduisant l'ordinal*

$$\varepsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\},$$

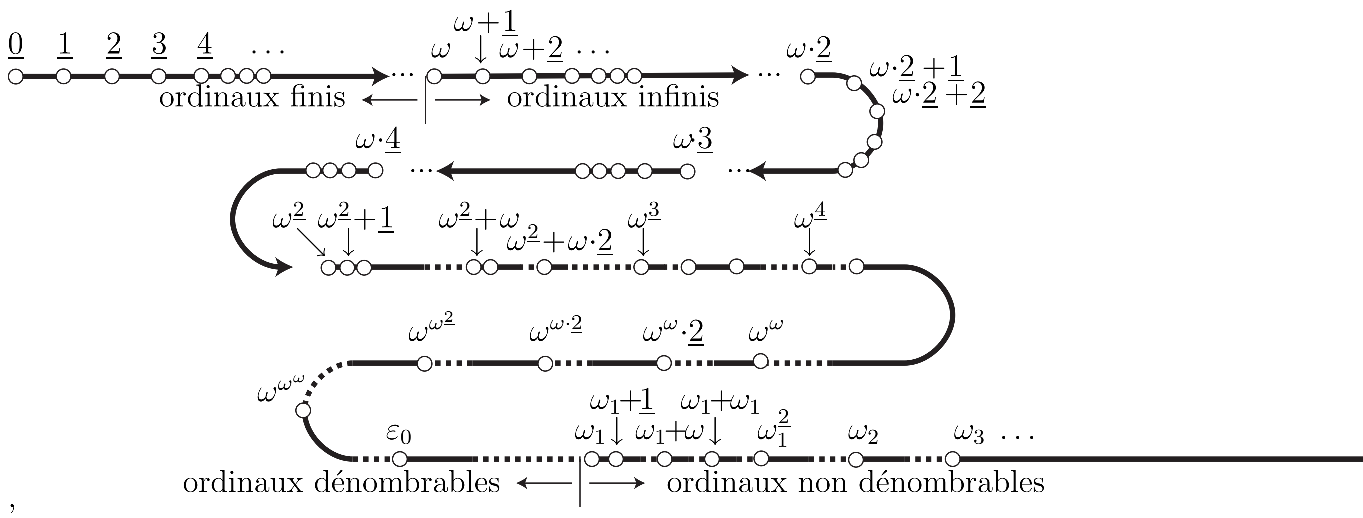
qui apparaît gigantesque. Pour autant, tous les ordinaux précédents, y compris ε_0, restent relativement petits puisque, en tant qu'ensembles, ils sont dénombrables. En effet, les arguments rappelés au chapitre I montrent que, si A et B sont des ensembles dénombrables, il en est de même des ensembles $A \uplus B$, $A \times B$, et $A^{(B)}$. Par contre, de même qu'elle a permis d'introduire *l'ordinal ω comme borne supérieure de tous les ordinaux finis, la proposition 2.16 permet d'introduire des ordinaux non dénombrables qui dominent tous les ordinaux dénombrables.* ◁

Proposition 3.20. (non injection) *Pour chaque ordinal infini α, l'ensemble des ordinaux s'injectant dans α est un ordinal, et c'est le plus petit ordinal qui ne s'injecte pas dans α.*

Démonstration. Soit Θ l'ensemble des ordinaux s'injectant dans α, c'est-à-dire l'ensemble des ordinaux qui sont en bijection avec α ou avec un ordinal inférieur à α. Posons $\theta = \bigcup\Theta$. Alors θ est un ordinal. Par hypothèse, Θ contient au moins un ordinal infini, à savoir α. Si β est un ordinal infini, l'application définie par $f(\underline{0}) = \beta$, $f(\underline{n}) = \underline{n-1}$ pour $n \geqslant 1$ et $f(\gamma) = \gamma$ pour $\gamma \geqslant \omega$ est une bijection de β sur $S(\beta)$. Donc $\beta \in \Theta$ entraîne $S(\beta) \in \Theta$. Par conséquent, Θ n'a pas de plus grand élément, et donc il ne contient pas sa borne supérieure, qui est θ. C'est dire que θ n'est pas dans Θ, donc qu'il ne s'injecte pas dans α, et c'est le plus petit ordinal ayant cette propriété puisque, par définition, tous les prédécesseurs de θ sont dans Θ. □

Notation 3.21. (figure 15) On pose $\omega_0 = \omega$, puis, de proche en proche, on définit ω_{n+1} comme le plus petit ordinal qui ne s'injecte pas dans ω_n.

▷ *Par exemple, ω_1 est le plus petit ordinal qui ne s'injecte pas dans ω, c'est-à-dire n'est ni fini, ni dénombrable. Par la proposition ci-dessus, ω_1 est la borne supérieure de l'ensemble des ordinaux finis ou dénombrables. Comme tout ordinal fini est inférieur à tout ordinal dénombrable, ω_1 est également la borne supérieure de l'ensemble des ordinaux dénombrables. De même, ω_2 est la borne supérieure de l'ensemble des ordinaux s'injectant dans ω_1, lesquels se composent des ordinaux finis, suivis des ordinaux dénombrables, suivis des ordinaux en bijection avec ω_1. Par conséquent, ω_2 est aussi la borne supérieure des ordinaux en bijection avec ω_1.* ◁



,

Figure 15. La suite des ordinaux (6) : au-delà de tous les ordinaux dénombrables commencent les ordinaux non dénombrables, inaccessibles par les opérations arithmétiques : ω_1, ω_2, ...

4. Deux applications

▶ Deux applications des ordinaux sont établies, à savoir le théorème de Cantor–Bendixson sur la structure des fermés de $\mathbb{R}$ en topologie, et le théorème de Goodstein sur la convergence des suites éponymes en arithmétique. ◀

▷ *Les ordinaux et leur arithmétique constituent une extension de l'arithmétique, un prolongement au-delà du fini de la suite des entiers naturels. La possibilité de compter avec des nombres transfinis préservant la propriété de bon ordre est un outil puissant. Il existe deux modes d'utilisation principaux des ordinaux, à savoir dans des définitions récursives où ils fournissent un ensemble d'indices plus long que les entiers mais néanmoins bien ordonné, et dans des arguments de terminaison : pour montrer qu'un processus P sur un ensemble A se termine en un nombre fini d'étapes, il suffit d'associer un ordinal à chaque élément de A qui diminue strictement sous l'action de P. On illustre ici chacun de ces modes sur un exemple.* ◁

4.1. Le théorème de Cantor-Bendixson.

▶ Démontré en 1883 par Cantor et par Bendixson, le résultat affirme l'existence pour tout fermé de $\mathbb{R}$ d'une décomposition en un ensemble dont tout point est point d'accumulation et un ensemble dénombrable. ◀

▷ *Ici les ordinaux sont utilisées à construire récursivement une suite de longueur ω_1, c'est-à-dire non dénombrable. On souhaite extraire d'un ensemble un ensemble dont tous les points soient points d'accumulation. L'idée est simple : on retire les points isolés. Ce faisant, de nouveaux points isolés peuvent apparaître, et il faut itérer le processus. Mais une itération indexée par les entiers ne suffit pas, et il faut poursuivre l'itération au-delà de ω.* ◁

Définition 4.1. (parfait) Un espace topologique est dit *parfait* si tout point est point d'accumulation.

Proposition 4.2. (théorème de Cantor–Bendixson) *Tout fermé de $\mathbb{R}$ est réunion d'un ensemble parfait et d'un ensemble fini ou dénombrable.*

Démonstration. Pour X inclus dans $\mathbb{R}$, notons ∂X l'ensemble des points d'accumulation de X. Si X est fermé, on a $\partial X \subseteq X$, et dire que X est parfait signifie qu'on a $\partial X = X$. Fixons une numérotation $U_1, U_2, ...$ des intervalles ouverts de $\mathbb{R}$ à extrémités rationnelles, et, pour x dans $X \setminus \partial X$, posons $p(x, X) := \inf\{p\,;\, U_p \cap X = \{x\}\}$. Alors $x \mapsto p(x, X)$ est injective puisque, pour $y \neq x$, on a $x \in U_{p(x,X)}$ et $y \notin U_{p(x,X)}$. Il en résulte que $X \setminus \partial X$ est au plus dénombrable.

Soit F un fermé. On construit par récurrence une suite de fermés de $\mathbb{R}$ indexée par les ordinaux en posant [7]

$$F_{\underline{0}} := F, \quad F_{\alpha+\underline{1}} := \partial F_\alpha, \quad F_\lambda := \bigcap_{\alpha<\lambda} F_\alpha \quad \text{pour } \lambda \text{ limite.}$$

Comme F est fermé, la suite est décroissante pour l'inclusion (au sens large). Pour chaque ordinal α tel que $F_\alpha \setminus F_{\alpha+\underline{1}}$ soit non vide, soit $p(\alpha) := \inf\{p(x, F_\alpha)\,;\, x \in F_\alpha \setminus F_{\alpha+\underline{1}}\}$. Supposons $\alpha < \beta$, et $p(\alpha), p(\beta)$ définis. Comme F_β est inclus dans $F_{\alpha+\underline{1}}$, aucun des points de F_β n'est dans $F_\alpha \setminus F_{\alpha+\underline{1}}$, donc on a certainement $p(\beta) \neq p(\alpha)$, et donc la famille des ordinaux α vérifiant $F_\alpha \setminus F_{\alpha+\underline{1}} \neq \emptyset$ est au plus dénombrable. Par conséquent, il existe un ordinal dénombrable θ

[7] On a montré que les ordinaux forment une suite bien ordonnée, ce qui légitime le principe des démonstrations par induction ordinale ; on utilise ci-après une construction par récursion ordinale, dont la légitimité découle, mais au prix d'une vérification qui ne sera donnée qu'au chapitre III ; la démonstration en cours est donc anachronique.

vérifiant $F_\theta = F_{\theta+\underline{1}}$, c'est-à-dire $F_\theta = \partial F_\theta$. On a alors $F = F_\theta \cup \bigcup_{\alpha<\theta}(F_\alpha \setminus F_{\alpha+\underline{1}})$. Par construction, F_θ est parfait, tandis que le second terme, union dénombrable d'ensembles dénombrables, est dénombrable. □

▷ *Le théorème de Cantor–Bendixson montre que l'hypothèse du continu est vraie pour les fermés. En effet, il est facile de vérifier qu'un sous-ensemble parfait de $\mathbb{R}$ est en bijection avec $\mathfrak{P}(\mathbb{N})$, donc avec $\mathbb{R}$. Par conséquent, si F est un fermé de $\mathbb{R}$, il s'écrit $F = P \cup D$ avec P parfait et D fini ou dénombrable : ou bien P est vide, et F est au plus dénombrable, ou bien P est non vide, et F est en bijection avec $\mathbb{R}$.* ◁

4.2. Suites de Goodstein.

▶ Les suites de Goodstein sont des suites d'entiers définies par une récurrence simple à partir de la notion de développement en base p itérée. Le théorème affirme que, paradoxalement, la suite atteint la valeur 0, alors que les premières valeurs suggèrent une croissance rapide vers l'infini. ◀

▷ *Il s'agit d'utiliser les ordinaux comme moyen de montrer la terminaison d'un processus. Ici, il s'agit de nombres entiers et de transformations qui, par construction, ne s'arrêtent que si la valeur 0 est atteinte. On démontre la terminaison en attachant un ordinal à chaque étape du processus de façon à ce que les ordinaux décroissent strictement aussi longtemps que la valeur 0 n'est pas atteinte. Comme il n'existe pas de suite infinie décroissante d'ordinaux, la seule possibilité est que la valeur finale 0 soit atteinte en un nombre fini d'étapes.*

Noter que, pour ce type d'application, n'importe quel bon ordre — ou même n'importe quelle relation bien fondée — peut être utilisé à la place des ordinaux ; au moins pour ce qui est des bons ordres, cette remarque ne change pas la portée de la méthode puisque tout bon ordre est isomorphe à un ordinal. ◁

Ecrire un entier n en base p consiste à décomposer n sous forme d'une somme décroissante

$$n = p^{n_1} \cdot c_1 + \cdots + p^{n_k} \cdot c_k$$

où les chiffres c_i sont compris entre 1 et $p-1$, et où les exposants n_i sont des entiers, nécessairement strictement inférieurs à n. On peut alors exprimer les exposants n_i eux-mêmes en base p, et itérer le processus. On appellera représentation de n *en base p itérée* la décomposition ainsi obtenue : par définition, il s'agit d'exprimer n au moyen des entiers 1 à $p-1$, de la somme, des $p-1$ multiplications par 1, … , $p-1$, et de l'exponentiation de base p.

Exemple 4.3. (base p itérée) Soit $n = 26$. La décomposition de n en base 2 est $26 = 2^4 + 2^3 + 2^1$: la décomposition de 4 est $4 = 2^2$, celle de 3 est $3 = 2^1 + 1$, et, finalement, la décomposition de 26 en base 2 itérée est $2^{2^{2^1}} + 2^{2^1+1} + 2^1$. De même, sa décomposition en base 3 itérée est $3^2 \cdot 2 + 3 \cdot 2 + 2$ [8].

Définition 4.4. (suites de Goodstein) (i) Pour $q \geqslant p \geqslant 2$, on définit une fonction $f_{p,q}$ de $\mathbb{N}$ dans $\mathbb{N}$ comme suit : $f_{p,q}(n)$ est l'entier obtenu en formant la décomposition de n en base p itérée, en y remplaçant partout p par q, et en évaluant le résultat.

[8] Pour 2, on a écrit 2^1 dans le cas de la base 2 itérée, car 2 n'est pas un chiffre en base 2, alors qu'on a écrit simplement 2 dans le cas de la base 3, car 2 est alors un chiffre, c'est-à-dire un entier plus petit que la base choisie

(*ii*) Pour chaque entier a, on définit une suite d'entiers $g_2(a), g_3(a), \ldots$ en partant de $g_2(a) := a$ puis en posant inductivement

$$g_{p+1}(a) = f_{p,p+1}(g_p(a)) - 1$$

si $g_p(a)$ est non nul, et $g_{p+1}(a) = 0$ si $g_p(a)$ est nul.

Exemple 4.5. (suites de Goodstein) Pour les fonctions $f_{p,q}$, on trouve par exemple :

$f_{3,4}(26) = f_{3,4}(3^2 \cdot 2 + 3 \cdot 2 + 2) = 4^2 \cdot 2 + 4 \cdot 2 + 2 = 42,$

$f_{2,3}(26) = f_{2,3}(2^{2^{2^1}} + 2^{2^1+1} + 2^1) = 3^{3^{3^1}} + 3^{3^1+1} + 3^1 = 3^9 + 3^4 + 3 = 19767.$

Considérons alors la suite de Goodstein pour $a = 5$. On part de $g_2(5) = 5 = 2^{2^1}+1$. On a ensuite $g_3(5) = f_{2,3}(5) - 1 = (3^{3^1} + 1) - 1 = 27 = 3^{3^1}$, puis, successivement,

$g_4(5) = f_{3,4}(27) - 1 = (4^{4^1}) - 1 = 255 = 4^3 \cdot 3 + 4^2 \cdot 3 + 4^1 \cdot 3 + 3,$

$g_5(5) = f_{4,5}(255) - 1 = (5^3 \cdot 3 + 5^2 \cdot 3 + 5^1 \cdot 3 + 3) - 1 = 447 = 5^3 \cdot 3 + 5^2 \cdot 3 + 5^1 \cdot 3 + 2,$

$g_6(5) = f_{5,6}(447) - 1 = (6^3 \cdot 3 + 6^2 \cdot 3 + 6^1 \cdot 3 + 2) - 1 = 775 = 6^3 \cdot 3 + 6^2 \cdot 3 + 6^1 \cdot 3 + 1,$

et la suite des $g_p(5)$ continue ainsi à croître résolument.

Et, pourtant, on a le résultat suivant :

Proposition 4.6. (théorème de Goodstein) *Pour tout entier a, la suite des entiers $g_p(a)$ converge vers 0 : il existe un entier p vérifiant $g_p(a) = 0$.*

Démonstration. L'argument est extrêmement simple à partir du moment où on peut utiliser l'arithmétique ordinale. Pour cela, nous introduisons, pour chaque entier p, une fonction $f_{p,\omega}$ de $\mathbb{N}$ dans les ordinaux sur le modèle de $f_{p,q}$: $f_{p,\omega}$ est l'ordinal obtenu en écrivant n en base p itérée, puis en remplaçant chaque entier k plus petit que p par $\underline{k}$ et chaque entier p par ω. Ainsi, par exemple, on a

$$f_{2,\omega}(26) = f_{2,\omega}(2^{2^2} + 2^{2+1} + 2) = \omega^{\omega^\omega} + \omega^{\omega+1} + \omega.$$

Supposons démontré que chaque application $f_{p,\omega}$ est croissante. Pour $p \geqslant 2$, on pose $\widetilde{g}_p(a) = f_{p,\omega}(g_p(a))$. Pour chaque entier a, on a ainsi une suite d'ordinaux $\widetilde{g}_2(a), \widetilde{g}_3(a), \ldots$. Or, par contruction, on a, pour tout p tel que $g_p(a)$ soit non nul,

$$\begin{aligned}\widetilde{g}_{p+1}(a) = f_{p+1,\omega}(g_{p+1}(a)) &= f_{p+1,\omega}(f_{p,p+1}(g_p(a)) - 1)\\ &< f_{p+1,\omega}(f_{p,p+1}(g_p(a))) = f_{p,\omega}(g_p(a)) = \widetilde{g}_p(a).\end{aligned}$$

En effet, pour tout n, on a $f_{p+1,\omega}(f_{p,p+1}(n)) = f_{p,\omega}(n)$, de même que, plus généralement et par construction, on a $f_{q,r}(f_{p,q}(n)) = f_{p,r}(n)$ quels que soient p, q, r vérifiant $2 \leqslant p \leqslant q \leqslant r$. Comme il n'existe pas de suite infinie décroissante d'ordinaux, il doit exister un entier p tel que $g_p(a)$ soit nul (figure 16). □

Il ne reste donc qu'à montrer le résultat auxiliaire suivant :

Lemme 4.7. *Pour tout p et tout n, on a $f_{p,\omega}(n) < f_{p,\omega}(n + 1)$.*

Démonstration. On fixe p au moins égal à 2, et on montre le résultat par induction sur n. Pour $n = 0$, on a $f_{p,\omega}(n) = \underline{0}$, et $f_{p,\omega}(n + 1) = \underline{1}$, donc le résultat est vrai. Supposons $n > 0$. Décomposons n sous la forme

$$n = p^{n-1} \cdot c_{n-1} + \cdots + p^1 \cdot c_1 + p^0 \cdot c_0,$$

$$\begin{tikzcd}
\widetilde{g}_2(a) \arrow[r, equal] & \widetilde{g}_2(a) \arrow[r, "{>}"] & \widetilde{g}_3(a) \arrow[r, equal] & \widetilde{g}_3(a) \arrow[r, "{>}"] & \widetilde{g}_4(a) \arrow[r, equal] & \dots \\
g_2(a) \arrow[u, "f_{2,\omega}"'] \arrow[r, "f_{2,3}"'] & \bullet \arrow[u, "f_{3,\omega}"'] \arrow[r, "-1"'] & g_3(a) \arrow[u, "f_{3,\omega}"'] \arrow[r, "f_{3,4}"'] & \bullet \arrow[u, "f_{4,\omega}"'] \arrow[r, "-1"'] & g_4(a) \arrow[u, "f_{4,\omega}"'] \arrow[r] & \dots
\end{tikzcd}$$

FIGURE 16. Démonstration du théorème de Goodstein : en bas, les entiers, en haut, leurs images chez les ordinaux infinis, qui gomment les changements de base ; ne restent alors que les -1 qui forcent la décroissance aussi longtemps que 0 n'est pas atteint.

où les coefficients c_k sont compris entre 0 et $p-1$. Par définition, on a

$$f_{p,\omega}(n) = \omega^{f_{p,\omega}(n-1)} \cdot \underline{c_{n-1}} + \cdots + \omega^{f_{p,\omega}(1)} \cdot \underline{c_1} + \omega^{f_{p,\omega}(0)} \cdot \underline{c_0} \tag{4.1}$$

Soit m le plus petit entier tel que le coefficient c_m ne soit pas égal à $p-1$. Alors, par construction, on a

$$n+1 = p^{n-1} \cdot c_{n-1} + \cdots + p^m \cdot (c_m + 1),$$

d'où

$$f_{p,\omega}(n+1) = \omega^{f_{p,\omega}(n-1)} \cdot \underline{c_{n-1}} + \cdots + \omega^{f_{p,\omega}(m)} \cdot (\underline{c_m} + \underline{1}). \tag{4.2}$$

Posons $\alpha = \omega^{f_{p,\omega}(n-1)} \cdot \underline{c_{n-1}} + \cdots + \omega^{f_{p,\omega}(m)} \cdot \underline{c_m}$, $\gamma = f_{p,\omega}(m)$, $\gamma_{m-1} = f_{p,\omega}(m-1)$, ... , $\gamma_0 = f_{p,\omega}(0)$ (donc $\gamma_0 = \underline{0}$). D'après (4.1) et (4.2), on a

$$f_{p,\omega}(n) = \alpha + \omega^{\gamma_{m-1}} \cdot \underline{c_{m-1}} + \cdots + \omega^{\gamma_0} \cdot \underline{c_0}, \quad f_{p,\omega}(n+1) = \alpha + \omega^{\gamma}.$$

Par hypothèse d'induction, on a $\gamma > \gamma_1 > \ldots > \gamma_m$. Alors des applications répétées de la proposition 3.18 donnent

$$\omega^{\gamma_{m-1}} \cdot \underline{c_{m-1}} + \cdots + \omega^{\gamma_0} \cdot \underline{c_0} < \omega^{\gamma},$$

d'où $f_{p,\omega}(n) < f_{p,\omega}(n+1)$ en ajoutant α à gauche. □

▷ *Le point essentiel dans la démonstration précédente est l'existence de l'ordinal ω, c'est-à-dire l'existence d'un nombre transfini qui domine tous les entiers à la façon dont ω le fait, donc en gros qui soit tel que la distance de 3 à ω soit la même que celle de 2 à ω. On utilise également l'existence d'une arithmétique cohérente et d'un bon ordre sur ces nombres transfinis, mais ces éléments apparaissent en quelque sorte gratuitement lorsqu'on construit les ordinaux comme ici. Reste donc l'existence de l'ordinal ω lui-même, qui n'est peut-être pas si bénigne que l'intuition semble le dire d'abord. On y reviendra.* ◁

Exercices

EXERCICE 1. (anti bon ordre) On suppose que $(A, <)$ est un ensemble bien ordonné, et que $(A, >)$ est aussi un ensemble bien ordonné, c'est-à-dire que toute partie non vide de A possède un plus petit et un plus grand élément. Montrer que A est fini. [Utiliser la proposition 1.18.]

EXERCICE 2. (bon ordre) On suppose que $(A, <)$ est un ensemble bien ordonné. On définit une relation $\prec$ sur $\mathfrak{P}(A)$ par $X \prec Y \Leftrightarrow \min(X \vartriangle Y) \in Y$, où $\vartriangle$ désigne la différence symétrique. Montrer que $\prec$ est un ordre total strict. Est-ce nécessairement un bon ordre?

Exercice 3. (ordres denses) Supposons que $<$ est un ordre total sur A. On dit que $<$ est *dense* si, toutes les fois qu'on a $a < b$, il existe c vérifiant $a < c < b$.

(i) Montrer qu'un bon ordre n'est jamais dense.

(ii) Montrer que tout ordre dénombrable dense sans minimum ni maximum est isomorphe à l'ordre des rationnels. [Supposant $(A, <)$ dénombrable, dense, sans minimum ni maximum, on fixe une numérotation des éléments de A, soit a_0, a_1, ... , et une numérotation des rationnels, soit q_0, q_1, ... Construire inductivement un isomorphisme f de $(A, <)$ sur $(\mathbb{Q}, <)$ comme suit : à la $2i$-ième étape, on regarde l'élément a_i de plus petit indice pour lequel $f(a_i)$ n'a pas encore été défini, et on pose $f(a_i) = q_j$, où j est minimal tel que q_j n'est pas encore dans l'image de f et a_i et q_j vérifient les mêmes contraintes d'ordre par rapport aux valeurs déjà définies de f; à la $2i + 1$-ième étape, on fait de même en considérant le premier rationnel q_j non encore dans l'image de f, et en posant $f^{-1}(q_j) = a_i$, où i est minimal tel que a_i n'est pas encore dans le domaine de f et a_i et q_j vérifient les mêmes contraintes d'ordre par rapport aux valeurs déjà définies de f.]

Exercice 4. (somme d'ordres) Soit $(A, <)$ un ensemble ordonné, et a un élément de A. Montrer que $(A, <)$ est isomorphe à la somme de $(I_<(a), <)$ et de $(A \setminus I_<(a), <)$.

Exercice 5. (transitif) Montrer que, si A et B sont des ensembles transitifs, il en est de même de $A \cup B \cup \{A, B\}$.

Exercice 6. (rang) On pose $V_0 = \emptyset$, et, inductivement, $V_n = \mathfrak{P}(V_{n-1})$ pour $n \geqslant 1$. Montrer que chaque ensemble V_n est transitif et qu'on a $\bigcup V_n = V_{n-1}$ pour $n \geqslant 1$.

Exercice 7. (indécomposable) Soit α un ordinal au moins égal à $\underline{2}$. Montrer qu'il y a équivalence entre (i) Pour tous $\beta, \gamma < \alpha$, on a $\beta + \gamma < \alpha$; (ii) Pour tout $\beta < \alpha$, on a $\beta + \alpha = \alpha$. (On pourra considérer séparément le cas où α est successeur et celui où il est limite). Montrer que ces propriétés sont vraies pour $\alpha = \omega$ et $\alpha = \omega^2$.

Exercice 8. (ordinaux limites) Montrer qu'un ordinal α est limite si et seulement si il existe β non nul tel qu'on ait $\alpha = \omega \cdot \beta$.

Exercice 9. (forme normale de Cantor) (i) Montrer que, si α est un ordinal non nul, il existe un unique ordinal β tel qu'on ait $\omega^\beta \leqslant \alpha < \omega^{\beta+\underline{1}}$.

(ii) En déduire que tout ordinal non nul admet une unique expression de la forme $\omega^{\alpha_1} \cdot k_1 + \cdots + \omega^{\alpha_n} \cdot k_n$ avec n entier, $\alpha_1 > \ldots > \alpha_n$ et $k_1, \ldots, k_n$ des entiers non nuls.

(iii) Montrer un résultat analogue en remplaçant ω par un ordinal γ quelconque, et les facteurs k_i par des ordinaux $\beta_i < \gamma$.

Exercice 10. (suites de Goodstein) Calculer le plus petit entier p vérifiant $g_p(2) = 0$; même question pour $g_p(3)$, et pour $g_p(4)$.